Instituto Superior de Ciências Sociais e Políticas
UNIVERSIDADE DE LISBOA

U LISBOA | UNIVERSIDADE DE LISBOA

"Nova Pangeia – Ameaças Vindas do Ciberespaço"

Luis Alberto de Jesus Gaio Curvelo
Professor Doutor Carlos Pedro Gonçalves

Dissertação para obtenção de grau de Mestre em Estratégia

Lisboa
2014

ÍNDICE

ÍNDICE DE QUADROS E FIGURAS

GLOSSÁRIO

ACARS – Aircraft Communications Addressing and Reporting System

ADS-B - Automatic Dependent Surveillance-Broadcast.

CIA - Central Intelligence Agency

COTS - Commercial-Off-The-Shelf

DDOS - Distributed-Denial-Of-Service

DOS - Denial-Of-Service

EUA – Estados Unidos da América

FAD - Food and Drug Administration

FMS - Flight Management System

IC - Infraestruturas Críticas

ICE - Infraestrutura Crítica Europeia

ICN - Infraestruturas Crítica Nacional

IP - Internet Protocol

ISP - Internet Service Provider

NAP - Network Access Points

NATO - North Atlantic Treaty Organization

NSA - National Security Agency

NSP - Network Service Providers

OCDE - Organização para a Cooperação e Desenvolvimento Económico

OSI - Open Systems Interconnection

POP - Point of Presence

SCADA - Supervisory Control and Data Acquisition

SPAM- Sending and Posting Advertisement in Mass

SWOT - Strengths, Weaknesses, Opportunities, and Threats

TCP - Transmission Control Protocol

TIC - Tecnologias da informação e comunicação

UAV - Unmanned Aerial Vehicle

UE- União Europeia

Ilustração por: Ana Madalena Curvelo (5 anos); João Carlos Curvelo (9 anos)

"***Corruptio Optimi Pessima***."

A corrupção do ótimo é péssima.

AGRADECIMENTOS

Ao meu Pai e minha Mãe, obrigado pelo exemplo e ensinamentos, nunca vos conseguirei pagar a *fortuna* que me deram.

Á minha Cúmplice, Esposa e Mãe dos meus Filhos, João e Madalena, obrigada pelo tempo cedido, força, companheirismo e ajuda que sempre me ofereceram. Respiro-vos.

Á minha irmã Isabel e ao João, obrigado pelo apoio e ajuda.

Ao meu Orientador, Professor Doutor Carlos Pedro Gonçalves, mais do que um Farol para chegar a bom porto, um exemplo inexcedível de profissionalismo, sabedoria e transmissão entusiasmada de conhecimentos. É um privilégio maior poder privar e trabalhar consigo.

Ao Professor Victor Lopo Cajarabille, Sr. Almirante, obrigada pela ajuda inicial.

Ao Eng.º José Alegria, Diretor da Cybersecurity, Privacy e Business Continuity (DCY) da Portugal Telecom e ao Mr. Matan Efrima, Director de Business Development & Marketing at Verint Communications and Cyber Intelligence Solutions, obrigada pela forma gentil e abnegada como partilharam informação.

Aos: Eng.º Paulo Andrade Santos, Eng.º Eduardo Soeiro, Dr. Nuno Valença, Eng.ª Marisa Antunes, Eng.º Marco Reis, Dr. José Melo, Dr. Manfred Ferreira – Obrigado pela sempre animada troca de informações e reflexões.

RESUMO

O presente trabalho, tem como **Objeto de Estudo a** "**Nova Pangeia" e as "Ameaças vindas do Ciberespaço**".

Tendo como ponto de partida a "Deriva Continental", de Wegener (1975, p.88), onde se teoriza que os diversos continentes estiveram inicialmente unidos num único, a Pangea.

Apesar da separação ocorrida, podemos verificar fenómenos que parecem contrariar esse afastamento.

Se às noções, de "Aldeia Global" de Mcluhan (1962), "Pangeia 2" de Schäfer (2003, p.76) e "Regresso a Pangeia" de Rifkin (2014, p. 259) adicionarmos o ciberespaço e a interconexão por ele provocada, aproximando pessoas, apelando para a noção de construção de um território alargado, encontramos a "Nova Pangeia".

Desta forma num primeiro momento sistematiza-se a organização deste sistema, padronizando as suas principais ameaças e veículos usados para produzir dano, estabelecendo correlações entre ataques Cibernéticos e Convencionais.

Posteriormente estabelecem-se correlações entre Infraestruturas Críticas Nacionais e a Nova Pangeia, analisando a sua existência, ligações e principais ameaças.

Seguidamente, realiza-se uma avaliação estratégica de risco, para a Nova Pangeia e para os sistemas a ela interconectados que em conjunção com a análise do Estudo de Caso, da Estónia e exemplos relevantes ocorridos, permitiram deduzir contributos para a Estratégia, fundamentalmente na área da Segurança e para o processo de tomada de decisão Estratégica.

Palavras-chave: Estratégia, Nova Pangeia**,** Ciberespaço, Internet, Segurança, Ameaças.

ABSTRACT

The present work has as its study object "**The New Pangeia**" and the "**Threats coming from Cyberspace**".

Taking as a starting point the "Continental Drift" from Wegener (1975, p.88), where he theorizes that the various continents were initially united in one, called Pangea.

And despite the physical split occurred, is possible to verify certain phenomena's that are contradicting this separation.

If to the notions of "Global Village" by Mcluhan (1962), "Pangeia 2" from Schäfer (2003, p.76), "Return to Pangeia" from Rifkin (2014, p.259), we add cyberspace and the interconnection caused by it, approaching Peoples, and appealing to the notion of construction of one extended territory, we find the "New Pangeia".

The first phase of this work was to systematize the organization of this system, by standardizing their main threats, as well used means to produce damage, trying to establish correlations between conventional and cyber-attacks.

Thereafter establishing correlations between National Critical Infrastructures and the "New Pangeia", analyzing its existence, connections and mains threats.

Subsequently, making a strategic evaluation of risk either for New Pangeia and for other interconnected systems in conjunction with the analysis of the Estonian Case Study, and relevant examples occurred, allowed to deduct contributions to Strategy and Strategic decision making process.

Keywords: Strategy, New Pangaea, Cyberspace, Internet, Security, Threats

1. CAPÍTULO – INTRODUÇÃO

Wegener (1929) teorizou que os diversos continentes que atualmente conhecemos, inicialmente estiveram unidos num único a que chamou Pangea. Este continente único, primeiro por partição depois por separação, fragmentou-se, dando origem aos continentes que atualmente conhecemos.

Este movimento de "deriva continental" provocou necessariamente um maior afastamento entre as espécies, nomeadamente entre a espécie humana, acentuando distâncias. Muitos milhares de anos depois surgem fenómenos que parecem contrariar esse afastamento.

A explosão dos meios de comunicação em massa, a Globalização, a "Aldeia Global" de Mcluhan (1962) aproximam o indivíduo, como se do regresso à aldeia, à tribo, se tratasse, mas desta feita a uma aldeia Global, alargada e que cobre todo o planeta.

Se a esta união, adicionarmos o ciberespaço e a interconexão por ele provocada aproximando pessoas e apelando para a noção de construção de um território alargado, unido, um cibercontinente, encontramos a "**Nova Pangeia**", que, enquanto novo continente, encontra no ciberespaço o seu território, permitindo a formação de um sistema interconectado de interligação.

Também Schäfer (2003, p.76) sugere que a confluência de interesses poderosos, como a Tecnociência, que está a emancipar a humanidade dos continentes e oceanos. Em conjunto com as capacidades, como a rápida comunicação, ramificação de redes de comunicação e transporte, permitirá atenuar as barreiras físicas, aproximado o mundo e começando a criar uma unidade civilizacional no topo da fragmentação global.

Em linha com esta teoria, Rifkin (2014, p. 264) também nos fala do "Regresso a Pangeia" afirmando que esse regresso se faz: "através de uma sociedade global cada vez mais integrada".

Surge assim o presente trabalho, que tem como **Objeto de Estudo a** "**Nova Pangeia" e as "Ameaças vindas do Ciberespaço**".

A "**Nova Pangeia"** com a sua organização hipertextual, iminentemente criada pelo desenvolvimento tecnológico, e em especial pela Internet, encontra-se em constante transformação, configurando um sistema e um novo **ambiente estratégico** centro de múltiplas atividades, para além das de carácter tecnológico, social, económico, financeiro, cultural e político. Este espaço, que se tem tornado indispensável às sociedades modernas, transformou-se numa das suas maiores vulnerabilidades (Santos, 2009), nele proliferando oportunidades e ameaças.

Neste sentido procura-se apresentar com esta dissertação um contributo para os **Estudos Estratégicos**, fundamentalmente na área da **Segurança**, tendo esta investigação como objetivos gerais o reconhecimento dessas ameaças e sua respetiva **avaliação estratégica de risco**, quer para a **Nova Pangeia** quer para os sistemas a ela interconectados e que nesta investigação serão analisados na perspetiva da **Estratégia,** como processo de decisão e de ação, identificando potencialidades e vulnerabilidades, disputas, forças em presença e recursos utilizados no espaço e no tempo, visando obter um produto que, conjugado com outras variáveis, contribua também para o processo de **tomada de decisão Estratégica.**

Após os acontecimentos na Estónia e Geórgia, onde a Internet e as TI são usadas como elementos ativos em conflitos de variada ordem, podemos inferir que existem novos campos de batalha, novas ameaças, provenientes deste espaço cibernético, e na sua capacidade para afetar aquilo que constituem ameaças físicas convencionais, que poderão envolver a perda de vidas humanas e de bens materiais (Janczewski & Colarik, 2008).

Neste sistema em constante mutação, o impacto da criminalidade**,** do terrorismo e da guerra cibernética tem-se vindo a acentuar, criando ameaças com implicações nos domínios: económico, ambiental, geopolítico, societal e tecnológico [1] **.**

Interessará pois conhecer estes fenómenos, e enquadrar o seu substrato na **Estratégia e no processo de decisão estratégia.**

1.1. Definição do objeto de Estudo

O termo ***"Nova Pangeia***", objeto de investigação desta dissertação, surge também no seio da comunidade científica, quer associado à biologia, quer à ciência do ciberespaço e à ciberfilosofia[2].

No seio da biologia, surge como estando associada ao processo de globalização e ao impacto que a ação humana tem na perda da Biodiversidade e da diversidade regional, que ocorre através da ação de homogeneização dos sistemas e ecossistemas, com a substituição de espécies ou elementos nativos, por espécies exóticas que se generalizam, tal como descrito por McKinney (2005, pp. 119–129).

1 NOTA: Foi utilizada a nova nomenclatura do World Economic Forum e do Risks Interconnection Map Fonte: Hayashi, Chiemi; Gleicher, David; Ramseger, Florian; Campbell, Karen; Soo, Amey; Tonkin, Samantha; Wright, Andrew and Stefaner, Moritz (2012). Global Risks 2012 – Seventh Edition, Switzerland. World Economic Forum. EUA. Acedido em 6 de março de 2013. Disponível para consulta em: http://www.weforum.org/reports/global-risks-2012-seventh-edition.

2 Nota: ramo da filosofia que tem como objetivo estudar os problemas filosóficos associados ao ciberespaço e internet.

Por outro lado**,** no campo da ciência do ciberespaço e da ciberfilosofia (H. Moor &Terrell, 2003), recorre-se ao uso da noção de "**Nova Pangeia"** para tratar o ciberespaço, também como um sistema de interconexão com potencial global.

Desta forma, o presente trabalho incidirá sobre este objeto de estudo, procurando nele também identificar ameaças, avaliando o seu risco estratégico, quer para o sistema em si, objeto de estudo, quer para outros sistemas a ele interconectados com especial relevo para as suas Infraestruturas e bem como para as Infraestruturas Críticas Nacionais.

1.2. Relevância do Tema para os Estudos Estratégicos

Milhões de cidadãos em todo o mundo contam com o ciberespaço, para cooperarem e colaborarem, para além de assegurar a sua comunicação, para ter acesso a instituições públicas e privadas**,** a bens e serviços. A acelerada desmaterialização dos processos e consequente migração para o ciberespaço tornam este sistema cada vez mais importante na medida em que cada vez mais funções e serviços, dele dependem para assegurarem o seu bom funcionamento.

Também os Estados encontram na **Nova Pangeia**, novas formas de comunicarem e se relacionarem com os cidadãos, não só pela disponibilização de serviços anteriormente apenas disponíveis fisicamente, mas também usando este sistema como um pilar para o seu próprio desenvolvimento. Presentemente grande parte dos aspetos da Governação assentam nas tecnologias de informação e na **Nova Pangeia**, os Organismos de Estado estão ligados em rede, as forças de segurança e emergência dependem do seu bom funcionamento no dia-a-dia para melhor assegurarem as suas missões e operações.

Esta realidade estende-se às Forças Armadas, sendo que o ciberespaço pode inclusivamente ser encarado com uma dupla utilização, como recurso ou infraestrutura para suportar operações, ou como recurso defensivo ou ofensivo (Jabbour, 2010, pag. 64).

Como espaço de combate e guerra, proporciona aos adversários uma opção de baixo custo para atacar interesses globais e facilitar operações ou manobras de defesa ou ataque.

Como sistema alargado, a **Nova Pangeia** e o ciberespaço oferecem novos instrumentos de ataque e defesa capazes de negaram a superioridade nos domínios ditos tradicionais: terra, mar, ar e espaço

Nesta medida representa ameaças para a **Segurança dos Estados e Cidadãos**.

Pretende-se assim, com esta investigação apresentar um conjunto de contributos em termos dos **Estudos Estratégicos**, que melhor permitam conhecer este novo sistema, tipificando-o, e demonstrando a sua relevância para a **Estratégia**.

Identificando claramente as forças (recursos ou capacidades disponíveis), poderes em presença (capacidade de impor uma vontade utilizando ou ameaçando utilizar a força), atores e interesses em disputa e principais Riscos e Ameaças. Desta forma, avaliando o seu potencial e capacidade para produzirem efeitos quer no sistema **Nova Pangeia,** quer nos Sistemas a ela conectados.

Neste contexto interessa realizar uma **avaliação estratégica do risco** associado às novas ameaças vindas do ciberespaço, tentando aferir em que medida estas afetam os principais domínios (económico, ambiental, geopolítico, societal e tecnológico[3]), deduzindo contributos para os **Estudos Estratégicos fundamentalmente no domínio da Segurança.**

1.3. Questões de partida

A investigação realizada pretendeu encontrar respostas para as seguintes **questões de partida**:

- **Será possível Correlacionar Ataques Cibernéticos e Convencionais?**
- **Existem interdependências entre Infraestruturas Críticas Nacionais e a Nova Pangeia?**

Estas questões foram centrais para o desenvolvimento da investigação, orientando o trabalho e a pesquisa, no sentido de se encontrarem respostas para estas questões.

1.4. Objetivos propostos para a Investigação

Os **objetivos** principais a atingir são:

- Realizar a caracterização sistémica da "**Nova Pangeia**;
- Analisar as novas **ameaças e vulnerabilidades** provenientes do **ciberespaço**;
- Efetuar uma **Avaliação Estratégica** de **risco** quer para a **"Nova Pangeia"** quer para os sistemas a ela interconectadas;
- Aduzir contributos para os **Estudos Estratégicos** fundamentalmente no domínio da **Segurança**.

3 NOTA: o trabalho do World Economic Forum**,** acerca do Risks Interconnection Map, levou a um reorientar do discurso científico acerca do risco nos sistemas para uma classificação operativa em termos de domínios (económicos, geopolíticos etc.), assim não se trata tanto de uma avaliação de risco centrada num domínio específico mas**,** sim, de uma avaliação do risco em rede conceptualmente esquematizada a partir de diferentes domínios de risco: económico, ambiental, geopolítico, societal e tecnológico, conforme informação disponível no website: http://www.weforum.org/reports/global-risks-2012-seventh-edition, acedida em 7 de março de 2013.

1.5. Metodologia e Estrutura da Dissertação

Uma vez que a investigação que se pretende realizar será iminentemente teórica, tendo em conta o objeto de estudo apresentado "**Nova Pangeia**", a metodologia a seguir estará de acordo com o método qualitativo. Desta forma será inicialmente realizado um estudo exploratório (Santos, 1999), com base na leitura e revisão de fontes bibliográficas relevantes, quer do ponto de vista da Estratégia quer do ponto de vista da temática envolvente ao objeto de estudo.

Esse trabalho é apoiado por consulta a fontes bibliográficas, análises documentais, consultas a artigos científicos, material produzido por organizações internacionais relevantes no setor (Governamental, Defesa, Segurança e Tecnologias de Informação) e seus respetivos documentos oficiais, consulta a fontes on-line, artigos e relatos de situações ocorridas.

A pesquisa é orientada numa perspetiva ex-post facto, com a identificação de situações já ocorridas e de importância específica para o tema da investigação, recorrendo ainda à construção de cenários de risco, manipulando-se variáveis por forma a ilustrar de que modo ou com que causas a situação foi gerada e que impactos pode produzir.

Como primeira tarefa, em termos metodológicos, procurou-se identificar e tipificar as novas ameaças geradas pela "**Nova Pangeia**", a partir de um processo de revisão dos principais padrões e dinâmicas associadas aos ataques cibernéticos. Através de uma sistematização e análise de casos exemplares, generalizáveis em termos de conclusões, encontraram-se padrões ou semelhanças que permitiram enquadrar as referidas ameaças com as ameaças convencionais.

Como segunda tarefa, e por forma a enriquecer a investigação, recorreu-se ao método de Estudo de Caso, para análise da problemática central, aplicando-se a metodologia proposta por Yin (2009, p.3), para a realização e investigação de Estudos de Casos.

Com o Estudo de Caso da Estónia, selecionado pela sua importância, magnitude e riqueza de fontes, investiga-se os acontecimentos de Abril e Maio de 2007, demostra-se as consequências das ameaças cibernéticas em conjugação com outros casos exemplares revistos ao longo do trabalho avalia-se o impacto e importância das ameaças cibernéticas e as suas possíveis relações com as ameaças convencionais.

Como terceira tarefa, a partir de uma análise estratégica, procurou-se avaliar de modo integrado o risco estratégico associado à "**Nova Pangeia**", em particular, na vertente das suas infraestruturas e das infraestruturas críticas Nacionais, que através desta possam ser afetadas, apresentando-se um conjunto de contributos, estratégias, exemplos e práticas, que melhor identificam as ameaças cibernéticas e permitem uma melhor sensibilização, reflexão e resposta do ponto de vista da segurança.

Desta forma, este trabalho desenvolve-se ao longo de 5 capítulos, sendo o primeiro constituído pela parte introdutória, onde o trabalho é apresentado e a problemática exposta.

Seguidamente no Capítulo 2, tipifica-se e desenvolve-se o objeto de estudo estabelecendo um mapa conceptual que permita contextualizar o tema, identificando a sua origem, composição, importância e impacto. Procurou-se ainda, padronizar e correlacionar tipos de ataques cibernéticos e convencionais com base na sua caracterização sistémica.

Passando-se seguidamente a analisar a existência de correlações entre a "**Nova Pangeia**" e as infraestruturas Críticas Nacionais, respetivos meios utilizados para a tentativa de produção de dano e seu potencial impacto.

No Capítulo 3 identificam-se as ameaças associadas a ataques cibernéticos, avaliando o seu risco e identificado por intermédio de cenários as ameaças. Pretende-se assim efetuar uma avaliação estratégica de risco quer para a "**Nova Pangeia"** quer para os sistemas a ela interconectados.

No Capítulo 4, com o **Estudo de Caso da Estónia**, retiraram-se bases da sua evidência e eventuais implicações/danos que estes produziram, quer em termos físicos, quer em termos lógicos, ilustrando com uma situação real o potencial de risco que estas novas ameaças representam.

A dissertação finaliza-se com o Capítulo 5, em que são apresentadas as conclusões relativas ao tema desenvolvido.

2. CAPÍTULO - NOVA PANGEIA - ORGANIZAÇÃO SISTÉMICA E AMEAÇAS CIBERNÉTICAS

Neste Capítulo apresenta-se a organização sistémica da Nova Pangeia (Secção 2.1), assim como se determinam os principais padrões básicos dos ataques cibernéticos, verificando a sua correlações com ataques ditos convencionais (Secção 2.2 e 2.3). No final do Capítulo (Secção 2.4) demonstra-se a correlação entre Segurança Nacional e a Nova Pangeia, por intermédio da análise às Infraestruturas Críticas Nacionais e sua relação com este sistema.

2.1. ORGANIZAÇÃO SISTÉMICA

Partindo da teoria da "Deriva Continental" de Wegener (1975, p.88-97), e do seu livro a "Origem dos Continentes e Oceanos", onde teoriza que os atuais continentes, há acerca de 300 milhões de anos, formavam uma única massa, a que denominou Pangeia[4].

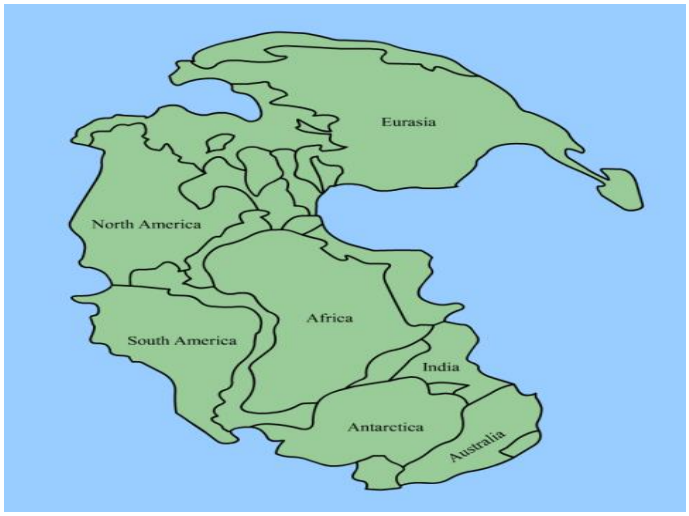


Figura 1 – Pangeia

(Fonte Imagem – thatthereengland – Disponível em: http://thatthereengland.wordpress.com/2013/09/29/our-current-world-redrawn-as-pangea/)

Esta massa que congregava todos os continentes, fragmentou-se e afastou-se, num longo processo de milhões de anos, até à configuração que hoje conhecemos.

Por analogia com a noção de Pangeia, assume-se a noção "**Nova Pangeia**", desta forma designada por conter em si, ligados em rede, todos os outros continentes, numa rede que embora seja formada por múltiplas redes, por via das suas conexões, age de forma a ser apenas uma, a Internet. A noção proposta de Nova Pangeia constitui uma expansão da noção de "Aldeia Global" proposta por Mcluhan (1962), que na década de 60 do século passado, teorizou como os meios de comunicação em massa, especialmente a Rádio, Televisão e

4 Nota: do grego pan/todo ou inteiro; Gaea/Terra.

sistemas de Satélite, permitiriam a abolição de fronteiras, reduzindo distâncias e garantindo um processo de comunicação mais rápido, a uma escala planetária**,** criando uma Aldeia Global, onde todos se conhecem e comunicam, emergindo assim um processo de retribalização da sociedade, ou o regresso do indivíduo a uma consciência coletiva, uma uniformização sociocultural, que nega o isolamento e o individualismo da destribalização, unindo a humanidade.

A proposta da noção de Nova Pangeia prende-se com a evolução ocorrida com o desenvolvimento do ciberespaço que permite uma interconexão com potencial para aproximar as pessoas ao invés de as distanciar, apelando assim para a noção de construção de um território, um cibercontinente, a "**Nova Pangeia**", que**,** enquanto novo continente, encontra no ciberespaço o seu território permitindo a formação de um sistema interconectado de interligação. A proposta da noção é convergente com Schäfer (2003, p.76-82) que aborda a história contemporânea a partir da noção que define como "verdadeiramente global". Distinguindo a história geofísica não-linear, que alternadamente vai unido e dividindo o "mundo-continente" a que chama de Pangeia UM, e a história tecnocientífica revolucionária da Pangeia DOIS, onde sugere que a confluência de interesses poderosos e capacidades, como a rápida comunicação, ramificação de redes de comunicação e transporte que surgem com base na tecnociência, estão a criar uma unidade civilizacional.

Também Rifkin (2014) na sua obra a "Terceira Revolução Industrial" propõe um regresso à Pangeia, tal como a internet liga a humanidade, num espaço, distribuído e colaborativo a Terceira Revolução Industrial, pretende ligar a espécie Humana num espaço político, paralelo semelhante à Pangeia. Esta Revolução, segundo Rifkin (2014), assenta em 5 pilares fundamentais:

1. Mudança para as energias renováveis;
2. Transformação das habitações e Imóveis em todos os continentes em micro plantas de geração de energias renováveis, que assegurem a produção local de energia;
3. Disseminação do hidrogénio e outras tecnologias de armazenamento em todos os Imóveis possibilitando o armazenamento de energias intermitentes;
4. Utilização da Internet, e suas tecnologias para transformar a rede elétrica de todos os continentes numa rede inteligente (Smart Grid), que permita gerir a energia para consumo e partilhar eventuais excessos de produção, para outros locais deficitários
5. Mudança das frotas de transporte para veículos elétricos e com células de combustível, possibilitando a comprar e venda de energia verde, em rede, de forma de interativa e a uma escala continental.

Com base nestes pilares e citando Rifkin (2014, p264) "Comunicação, energia e comércio global em rede originam, invariavelmente, uma administração em rede, quer a nível global, quer a nível continental. A engenharia de um espaço continental interligado cria uma nova

orientação espacial." Formando-se assim segundo o autor "uma sociedade global cada vez mais integrada, gerando-se um fenómeno de continentalização, sendo a União Europeia, um exemplo da primeira união continental (Rifkin 2014, p264 -266).

Tendo em atenção a ligação entre a noção de Nova Pangeia e o ciberespaço, importa rever a noção de ciberespaço cuja introdução se deve a Gibson (1983). O termo ciberespaço remete para a cibernética, logo, pode ser pensado enquanto espaço disponível para estruturas cibernéticas, as quais podem ser definidas a partir de redes dinâmicas de relações de gestão e organização entre sistemas que se servem da capacidade conectora do "espaço eletricamente contraído" para "alimentarem" a sua atividade, McLuhan (1962).

A definição original de ciberespaço encontra-se no livro Neuromancer de Gibson (1983)[5] é assumido pela comunidade científica com valor operativo para contextos empíricos. Esta remete para um conjunto de máquinas/sistemas, que globalmente são diariamente operados/manuseados por utilizadores. Essas máquinas/sistemas eletronicamente recebem, enviam e armazenam dados, num ambiente, rede ou sistema próprio que estabelece ligações complexas, em que a comunicação se dá de-um-para-um ou de-um-para-muitos, simétrica ou assimetricamente.

Assume-se assim a noção de "**Nova Pangeia**", cujo conceito se forma com base em: ***Pan* (todos) + *Gaia* (terra)** + ***Ciberespaço***: sistema organizado em rede, com causalidade interconetiva.

Porém, para podermos entender este sistema, teremos que olhar para ele do ponto de vista da sua genética e da sua estrutura, sendo necessário conhecer duas das suas principais componentes, uma que denominamos "**Sistema Físico**", que se centra fundamentadamente ao nível da infraestrutura, de onde se destaca a Internet, e outra componente que designamos "**Meio Lógico**", e que diz respeito às aplicações ou códigos que a rede transporta.

2.1.1. O "Meio Físico",

Não sendo a internet a única rede, ela é de longe a mais usada e disseminada em termos Globais, interessa pois conhecer melhor o seu meio "Meio Físico".

A própria arquitetura da Internet encontra-se descrita na palavra *internet*, um diminutivo de "*inter-networking*" ou inter-redes, trata-se, assim, de uma rede composta por milhares ou *N* outras redes individuais, que se encontram em constante mudança e atualização. Essas redes

5 Definição do Original "Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding..."Fonte: Gibson, William (1983). – Neuromancer. Vancouver. pag. 31, acedido em 8 de março de 2013, disponível para consulta em: http://www.hugocarrion.com/index_archivos/Docs/A_neuromancer.pdf

são intercomunicantes, estão ligadas entre si, e usam um protocolo comum para estabelecer a sua comunicação/ligação.

Podemos afirmar que a arquitetura da Internet é baseada na especificação do protocolo **TCP / IP – TCP** e **IP** standard, projetado para possibilitar a conexão de redes, heterogenias, diferentes em termos de *hardware*, *software* e topologia. Assim duas ou *N* redes interconectam-se, a comunicação via TCP / IP é estabelecida *end-to-end*, de modo que qualquer nó ligado na rede/Internet tem a capacidade de estabelecer a comunicação com qualquer outro nó, independentemente da sua localização física ou geográfica.

Podemos ainda estabelecer uma analogia, em termos de funcionamento desta arquitetura, com um grande rio, em que os seus pequenos e médios afluentes alimentam um rio maior, comunicante em todo o seu estuário.

Os diversos nós, ou dispositivos ligados na rede, para comunicarem entre si, têm de ter um endereço único, que obedece a um esquema: nnn.nnn.nnn.nnn onde nnn deve ser um número de 0-255 (Shuler, 2005). Este endereço é conhecido como o endereço **IP** (IP que, conforme referido, significa *Internet Protocol*) e que na maioria das redes existentes obedece à especificação IP Versão 4, sendo que nesta especificação**,** atualmente em uso o número de endereços encontra-se limitado a 2^{32}, situação que será ultrapassada com a massificação do uso do IP Versão 6, onde o número de endereços será de 2^{128}, que em conjunto com diversas técnicas de multiplexagem e transladação de endereços, afasta a eventual questão da escassez de endereços.

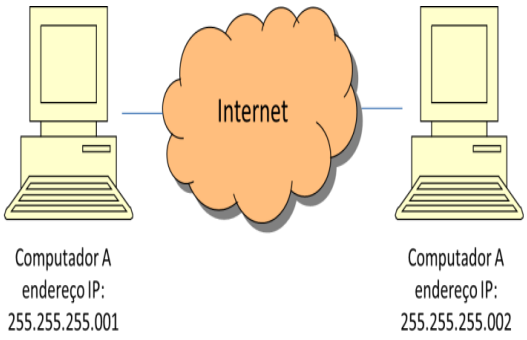


Figura 2 - Esquema de Endereçamento IP

(Fonte Imagem – Adaptado do livro - Engenharia de Redes Informáticas. FCA - Editora Informática)

Na Figura 2 - Esquema de Endereçamento IP temos dois computadores ligados à Internet, que através de endereços distintos podem comunicar entre si.

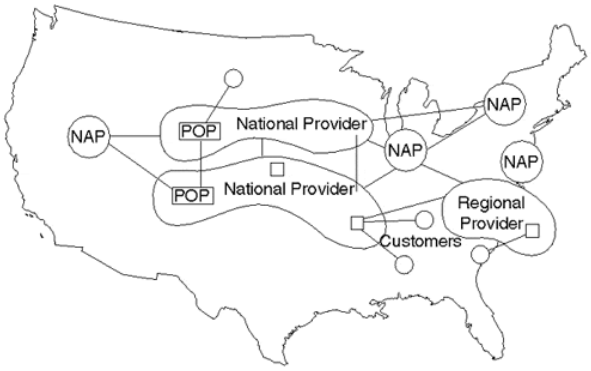


Figura 3 – Arquitetura da Internet

(Fonte Imagem – Retirada do livro – "Internet Routing Architectures", Cisco Press)

Do ponto de vista genérico, podemos enquadrar a Figura 3 Arquitetura da Internet (Halabi & McPherson, 2000) como representando a arquitetura da Internet contemporânea, sendo formada por um conjunto de:

Point of Presence (POPs), distribuídos por diversas regiões, que são pontos de conexão dos operadores, ou prestadores de serviços, normalmente denominados por **Internet Service Provider (ISP)**, este termo é geralmente utilizado quando se refere a quem fornece o serviço de Internet, seja diretamente para os utilizadores finais ou a outros fornecedores. Estes **POPs,** interligados entre si, formam as suas redes, e são os pontos por onde os clientes acedem aos serviços de Internet.

Dado que alguns prestadores de serviços de Internet podem apenas cobrir determinadas regiões geográficas, para permitir que os seus clientes ou os de um outro determinado prestador de serviço possam comunicar entre si, existem os ***Network Access Points*** **(NAPs)** que são pontos de interligação entre prestadores de serviço, ou entre redes, assegurando a ligação entre as várias redes e os seus utilizadores.

Neste contexto interessa clarificar o conceito: ***Network Service Providers*** **(NSPs)**, ou prestadores de serviços de rede que não fornecem serviços de Internet aos utilizadores finais, apenas prestam serviços para os operadores, alugam ou cedem a sua rede ou partes delas a terceiros para estes utilizarem. Um bom exemplo disso são as ligações submarinas entre continentes, ou os troços de comunicações realizados por satélites.

Mantendo a analogia com o rio, acabámos de descrever**,** do ponto de vista sistémico**,** como os canais funcionam, se ligam e estão organizados, teremos agora de falar dos conteúdos, ou seja**,** das aplicações que genericamente correm neste sistema.

2.1.2. O "Meio Lógico",

Para facilitar o entendimento deste meio, recorre-se ao modelo OSI (*Open Systems Interconnection*).

Modelo criado para estabelecer normas, que regulamentam a troca de informação entre sistemas, tendo como objetivo garantir que os sistemas comuniquem entre si, recorrendo ao uso de normas comuns, tal como refere Gouveia (1997).

Este modelo encontra-se distribuído por camadas (*layers*) hierárquicas com funções distintas, em que cada uma das camadas usa as funções da própria ou da camada anterior.

Estando organizado em 7 camadas, que asseguram a ligação entre Sistemas Lógicos e Físicos (Gouveia, 1997), tendo a composição apresentada na Figura 4 – Modelo OSI (Open Systems Interconnection):

Figura 4 - Modelo OSI (Open Systems Interconnection).

(Fonte Imagem – Adaptado do livro - Engenharia de Redes Informáticas. FCA - Editora Informática)

A normalização deste modelo permitiu estabelecer um conjunto de regras e procedimentos por parte dos fabricantes de hardware e software, que assegura que todos os dispositivos e aplicações conectados na rede possam comunicar entre si e trocar dados ou informações, respeitando a organização apresentada, sendo que as 7 camadas deste modelo OSI asseguram um conjunto de funções fundamentais conforme apresentadas no **Anexo - 7.1 Principais funções das camadas do modelo OSI.**

Apresentado o modelo, podemos definir, agora a componente lógica do sistema, ou o **software**, termo genérico que qualifica conjuntos organizados de dados informáticos e instruções, muitas vezes divididos em duas categorias principais: **software de sistema** que

fornece as instruções básicas ou rotinas específicas, funções ao computador e **software de aplicação** que é utilizado pelos utilizadores para realizar tarefas específicas.[6]

O software de sistema é responsável por controlar, integrar e gerir os componentes individuais de hardware de um sistema informático, para que outro software e os utilizadores do sistema possam vê-lo como uma unidade funcional sem terem que se preocupar com os detalhes de baixo nível, tais como a transferência de dados da memória para o disco, ou processamento de texto. Geralmente, o software de sistema consiste num sistema operativo e alguns utilitários fundamentais.

O software de aplicação[7], por outro lado, é utilizado para realizar tarefas específicas que não estão apenas adstritas à execução de instruções de sistema. O Software aplicacional pode consistir de um único programa, como um visualizador de imagens, ou conjunto de programas que funciona em conjunto para realizar tarefas, como o Microsoft Office, ou um sistema de gestão de base de dados. O software fornece uma variedade de outras aplicações independentes.

O software é criado com linguagens de programação e utilitários relacionados que podem existir em várias formas: programas simples, pacotes, compiladores, editores e outras ferramentas.

É a conjunção destes sistemas (Físico e Lógico) que permite obter a experiência de navegação na Internet, a visualização de um filme, a troca de mensagens ou execução de um programa de natureza diversa.

Por intermédio do software é possível que se possam propagar vírus informáticos, que são de forma genérica, programas de software que se propagam de um computador para outro, interferindo com o seu funcionamento. Um vírus informático pode danificar ou eliminar dados armazenados num computador, utilizar um programa de correio eletrónico para propagar o vírus para outros computadores ou mesmo eliminar tudo o que está armazenado no disco rígido[8].

Interessará pois conhecer como estes ataques se propagam.

6 Fonte: Universidade da Beira Interior. Noção de software. As aplicações WORD e EXCEL. Acedida em 7 Novembro de 2012 disponível para consulta em:
http://www.di.ubi.pt/~cbarrico/Disciplinas/Informatica/Downloads/Capitulo3.pdf
7 Fonte: Idem
8 Fonte: Microsoft (2011).Vírus informáticos: descrição, prevenção e recuperação. Artigo: 129972 - Fevereiro - Revisão: 2.1. acedido em 7 de Novembro de 2012 disponível em: http://support.microsoft.com/kb/129972/pt

2.2. Padrões Básicos dos Ataques Cibernéticos

Diferentes tipos de ataques cibernéticos podem ser realizados recorrendo ao uso de múltiplas tecnologias e técnicas, contudo, pode ser traçado um padrão básico de ataque faseado, que não obstante ser genérico é também aquele que é usado em termos da manobra subversiva, e que obedece na grande maioria dos casos ao modelo descrito por Janczewski (2007, Capítulo XV) apresentando o seguinte padrão:

- **Reconhecimento das Vítimas/Alvos**

  Esta fase implica uma observação primária das Vítimas/Alvos, sendo uma fase de aprendizagem, tenta-se acumular e apurar informação sobre os sistemas alvos a atacar, nomeadamente sobre as suas infraestruturas de *hardware* e *software*, tipologias de rede, tipos de comunicações utilizadas. Estas informações normalmente são correlacionadas com informações do tipo físico, no que diz respeito a políticas e procedimentos de segurança e modos de operação.

  Após a identificação dos pontos fortes e fracos, estudam-se cenários de ataque, procede-se a ações de captura ou penetração.

- **Penetração**

  A segunda fase de um ataque cibernético, normalmente, é a tentativa de penetração ou captura de informação.

  Nesta fase, os atacantes/invasores, visam a penetração ou a tentativa de captura de dados ou informações, que lhes permita ganhar vantagens ou diminuir a qualidade de serviço, ou até mesmo danificar ou inoperacionalizar sistemas. Nesta fase, prepara-se o dispositivo e "encontra-se a brecha", que permitirá avaliar as defesas do alvo.

- **Identificação de capacidades**

  A terceira fase consiste em identificar e aferir as capacidades internas dos alvos, visualizando os seus recursos e tentando penetrar em áreas mais reservadas ou sensíveis, dentro da rede e dos sistemas visados, aferindo centros de equilíbrio estratégico, que possam ser alvos dos ataques.

- **Produção do Dano**

  A quarta etapa é quando o intruso provoca o dano no sistema, ou "rouba" a informação que pretende.

A produção do dano está intimamente ligada à técnica ou ferramenta utilizada, normalmente varia consoante o tipo de objetivo, sendo que o dano pode ser provocado de forma isolada, ou de forma alargada a todos os sistemas ligados numa determinada rede.

Os mecanismos de atuação podem ser de natureza direta: quando normalmente o sistema utilizado para o ataque pertence ao atacante, no todo ou em parte, e nele são executadas as ações de ataque; ou de natureza indireta: quando o sistema, ou sistemas utilizados, são usados sem o conhecimento dos seus utilizadores, ou proprietários, sendo alvo de ativação e comando remotos.

- **Eliminação da Prova**

A última fase, na grande maioria dos ataques, destina-se à eliminação de qualquer evidência da intrusão, invasão, ou roubo. Tentando encobrir, ludibriar ou apagar o rasto/log, por forma a dificultar a identificação do intruso e as técnicas/ferramentas, por ele utilizadas.

2.2.1. Tipos de Ataque e veículos mais Utilizados

Segundo o Internet Crime Complaint Center (IC3) [9], no relatório de atividade referente a 31 de Dezembro de 2013, foram só nos EUA registadas 262.813 queixas/reclamações de crimes realizados on-line.

No mesmo ano, segundo a mesma fonte, estas denúncias representaram prejuízos de 781,841 milhões de dólares. Este número traduz a importância crescente dos prejuízos que este tipo de ataques pode causar, transmitindo uma ideia da sua importância.

Estes incidentes foram perpetrados, recorrendo ao seguinte tipo de ataques, mais comuns:

- **Ataques por Vírus ou Worms[10]**
- **Denial-Of-Service Attack (DOS attack) ou Distributed-Denial-Of-Service Attack (DDOS attack)[11]**

9 Fonte: acedido em 16 de Fevereiro de 2014. Relatório disponível para consulta em: http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

10 Nota: Ataques por Vírus ou Worms - Normalmente entregues via e-mail e contidos em anexos aparentemente pacíficos, podem também ser lançados por scripts (códigos ou guiões, que permitem executar um determinado conjunto de instruções, que ao serem invocados despoletam determinadas ações). Podem também estar alojados em sites que, com a passagem do browser, se propagam, explorando uma determinada vulnerabilidade.

11 Nota: Denial-Of-Service Attack (DOS attack) ou Distributed-Denial-Of-Service Attack (DDOS attack) - são ataques combinados, normalmente causados por aplicações do tipo "Trojan", aplicações escondidas em

- **Sites com Informação falsa ou alterada[12]**
- **Intrusão, Roubo, Alteração ou Destruição de Informação[13]**
- **Control Channel Attacks[14]**
- **Fuzzing[15]**
- **Ataques Unificados[16]**

No que diz respeito aos veículos de ataque ou formas de transmissão principais das ameaças podemos destacar:

- **Sites/Portais de Informação[17]**
- **E-Mail[18]**
- **Web Browser[19]**
- **Clientes de Chat[20]**

sistemas, que os utilizadores podem não ter informação de estarem contaminados e que atuam em data e hora pré-determinada, ou são remotamente invocados por um Hacker ou utilizador malicioso que, de forma coordenada, lança pedidos de resposta a um determinado alvo ou servidor, este último, confrontado com uma série de pedidos anormais de resposta, entra em colapso por não ter capacidade de processamento de resposta ou, como medida de proteção, desliga-se ou reinicia o serviço, gerando indisponibilidade.

12 Nota: Sites com Informação falsa ou alterada - Sites por exemplo informativos, ou de interesses comerciais ou governamentais, são utilizados em campanhas de desinformação, propaganda ou guerra psicológica. Basicamente, são alterados os seus conteúdos, de forma temporária ou permanente, com o objetivo de espalhar pânico ou gerar desinformação. Este tipo de técnica foi utilizado pelas forças Russas, no ataque à Geórgia, onde foram alterados diversos sites oficiais, com informação falsa, numa clara manobra de subversão e propaganda.

13 Nota:Intrusão, Roubo, Alteração ou Destruição de Informação – Este é um dos ataques, que em conjunto com o DoS attack, é o mais comum, sendo um dos mais perigosos, uma vez que que visa a intrusão, não autorizada, em sistemas, com o objetivo de roubo de informação confidencial ou informações proprietárias, alteração ou corrupção de dados e informação. Por outro lado, este tipo de ataque é o que permite uma interação com outros sistemas "físico" como os já descritos.

14 Nota: Control Channel Attacks – Ataques que visam tipicamente controlar ou causar disrupções ao nível do protocolo de comunicações impedindo sessões e desviando tráfego.

15 Nota: Geração de dados inválidos, imprevistos ou aleatórios direcionados a um sistema com objetivo de testar os seus acesso, embora seja uma técnica comummente utilizada para testar problemas de segurança, pode ser utlizada para explorar e encontrar falhas. Um tipo muito comum deste ataque é o SPIT- Spam Over Internet Telephony, basicamente trata-se de gerar tráfego falso visando uma infraestrutura de voz sobre IP com o objetivo de encontrar portos de entrada ou impedir o seu funcionamento pela exaustão de pedidos de resposta um pouco como o DDOS.

16 Nota: Ataques Unificados – São ataques que recorrem ao uso de uma ou mais técnicas de intrusão/disrupção de sistemas utilizando diversas técnicas em simulamento.

17 Nota: Sites/Portais de Informação – Sítios onde habitualmente os utilizadores interagem, consultam informação, submetem pedidos e executam ordens.

18 Nota: E-Mail – Programa de troca de mensagens e conteúdos eletrónicos, um dos principias veículos de transmissão de ameaças.

19 Nota: Web Browser – Aplicação que permite a consulta on-line a conteúdos e sítios na internet.

20 Nota: Clientes de Chat – Aplicações destinadas à troca de mensagens e conferências, de um-para-um, ou de um-para-muitos.

- **Remote Software**[21]
- **Web-Enabled Applications**[22]
- **Updates**[23]
- **Deliverables**[24]
- **Viruses and Worms**[25]
- **Trojans**[26]
- **Malicious Scripts**[27]
- **Suportes**[28]

Interessa ainda destacar que estes tipo de ataques podem ser "ubíquos" em termos do tipo de transporte utilizado, são quase como que se fossem universais em termos da estrutura utilizada de transporte e acesso, podem atingir os seus alvos, quer estejam a usar uma rede de dados fixa, de banda curta ou larga, de uma rede móvel ou de uma rede sem fios, transmitidas através de um smartphone, computador portátil, de um computador de secretária ou servidor. O seu potencial de dano não se limita a estes fatores, o que em termos táticos e estratégicos dificulta e torna mais sofisticadas, as operações de defesa ou de ataque.

21 Nota: Remote Software – Programa de ativação remota, por invocação, por alteração de estado ou por relógio.
22 Nota: Web-Enabled Applications – Programas desenhados e desenvolvidos de forma nativa para correrem na Internet.
23 Nota: Updates – Sistemas de atualização de programas, destinados primariamente a atualizar aplicações, ou a adicionarem novas funcionalidades, ou a corrigirem falhas.
24 Nota: Deliverables - Sistemas que podem ser explorados numa data posterior, tendo intenção de executarem instruções, normalmente descarregados em conjunto com outro tipo de aplicações e mediante invocação remota executam determinados comandos ou ações.
25 Nota: Viruses and Worms – Programas com base de código maligna, destinados a causar infeções no sistema, que visam explorar as vulnerabilidades. São de base intrusiva de ação rápida ou retardada, e na sua grande maioria são incluídos ou camuflados noutras peças de software.
26 Nota: Trojans – Tipo de aplicação, normalmente embutida num programa, aparentemente benigno, que depois de instalado no sistema se revela e cumpre outros fins, tais como abrir portas de comunicação com o exterior ou causar danos nos sistemas hospedeiros.
27 Nota: Malicious Scripts – Código que quando é executado pela aplicação ou sistema, produz efeitos maléficos nesse dito sistema. Este tipo de técnica é muito comum em aplicações de instalação ou visualização de conteúdos on-line, normalmente instala, por exemplo, loggers, pequenas aplicações que escutam o teclado e enviam informação para locais remotos, ou, abrem determinados portos no sistema, que normalmente estão fechados, facilitando a intrusão.
28 Nota: Suportes – Formas físicas ou lógicas que permitam o transporte de programas, dados ou informações, para além naturalmente das conexões em redes ou dispositivos de rede suportes como: memórias usb, cartões de memória, discos rígidos portáteis, entre outros, podem alojar ameaças off-line, e que mediante a interação com outros dispositivos, ou contacto em rede passam a on-line, ativando-se e transmitindo ou executando comandos ou instruções previamente estabelecidas, que permitem a ação em sistemas terceiros, para além deles mesmos.

2.3. Correlações entre Ataques Cibernéticos e Convencionais

No decorrer da história recente, encontramos alguns traços comuns e de interligação entre ataques cibernéticos e ataques convencionais. Com efeito, Janczewski (2007, Capítulo XIV) apresenta as seguintes semelhanças:

- ***Agressões convencionais são geralmente antecedidas de ataques cibernéticos:*** Antes mesmo dos ataques convencionais da Rússia contra a Geórgia em 2008, as operações já tinham começado no Ciberespaço, com ataques a sites governamentais da Geórgia e de várias empresas públicas e privadas[29].

- ***Os Ataques cibernéticos visam alvos que representem elevada importância em termos de opinião pública e meios de comunicação social:*** Os Ataques cibernéticos são realizados de forma a causar prejuízos graves e/ou a gerar elevada publicidade. Todas as instalações, associadas ao topo de unidades administrativas e militares, são alvos primários. Para além de organizações governamentais, ataques cibernéticos são lançados contra as empresas mais visíveis e dominantes, como as multinacionais. Os alvos preferidos pelos atacantes são empresas reconhecidas como fazendo parte das cem maiores empresas nos EUA, 27 foram em 2012 alvo de ataque (Dilpesh, 2009).

- ***O aumento dos ataques cibernéticos está relacionado com as causas políticas e fenómenos terroristas:*** Logo após a morte de Bin Laden foram lançados inúmeros ataques usando Trojans, como forma de retaliação pela sua morte (Computerworld, 2011).

29 Fonte: CCDCOE (2019). Cyber Attacks Against Georgia: Legal Lessons Identified. acedido em 17 de Fevereiro de 2014 Disponível para consulta on-line em:
http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

Ainda segundo Janczewski (2007, Capítulo XIV), podemos inferir que os ataques ou atos de guerra no ciberespaço estão intimamente relacionados com atos ou ações de guerra dita convencional.

A guerra da informação, ou os ataques cibernéticos, surgem como na guerra clássica; têm como base uma estratégia, a sua preparação desenvolvida recorrendo naturalmente a conhecimentos específicos, que se ajustam tendo em conta cenários ou operações a desenvolver, tendo assim dois campos fundamentais e que são comuns aos conflitos clássicos, ou seja**,** a ação ofensiva e ação defensiva.

Através da via ofensiva assume-se um percurso legítimo na justificação da opção, atribuir-se-á um valor aumentando para si na posse do recurso que se encontra em controlo do atacado e persuadir-se-á o seu opositor, aquele que defende (Bispo, 2001).

Enquanto a operação defensiva, valoriza a perda do que está em questão, sendo que o seu esforço está orientado em face daquele que queira capturar aquele recurso.

Esta valorização tem em conta o empenhamento, seja ele ofensivo (não tendo recurso), como defensivo (preservar um bem que se valoriza muito).

Assim, qualquer elemento do recurso informação pode constituir-se como alvo daquele que procura retirá-la ao seu possuidor, com o objetivo de ganhar uma vantagem nesse ou noutro campo, sendo nesta guerra a informação um ganho/perda típica do jogo. (Bispo, 2001)

Para um determinado ator, o valor do recurso informação é caraterizado em função de vários fatores (Bispo, 2001):

- Da relevância, de acordo com as preocupações e comprometimentos assumidos (o desejo em obter, fruto das circunstâncias e dos objetivos);
- Da capacidade do ator em extrair todas as potencialidades;
- Da disponibilidade do recurso para o ator e para os outros atores;
- Da integridade do recurso, no sentido de estar completo, de ser autêntico e de possuir as qualidades que se esperam que tenha;
- Do tempo ou da oportunidade.

A guerra da informação é valorizada na disputa, competição e conflito, em que os atores partilhem de forma semelhante os fatores enunciados, e que se manifestem a irredutibilidade e a inviabilidade do processo negocial pacífico.

Assim, as três componentes que a guerra de informação neste contexto abarca são:

- Uma que corresponde às ações para adquirir, processar e disseminar informação (exploração), no sentido de dominar numa determinada área (funcional/geográfica), contribuindo para obtenção de vantagem pelo ganho de conhecimento;
- Outra que protege o conhecimento adquirido e que constitui a componente das operações defensivas;
- E uma outra que ataca os sistemas do opositor para obter informação e assim ganhar uma vantagem, em diferencial de conhecimento e que são as operações ofensivas.

Como exemplo recente de Guerra de Informação, o Washington Post, na sua edição de 27 de Maio (Nakashima, 2013), divulga que muitos dos projetos de sistemas de armas avançadas dos EUA, os mais sensíveis, podem ter sido comprometidos por "Hackers"[30] Chineses, de acordo com um relatório preparado para o Pentágono e, funcionários do governo e da indústria de defesa.

Entre as mais de duas dezenas de grandes sistemas de armas cujos projetos foram violados, encontram-se programas críticos para as defesas de mísseis norte-americanos**,** aviões de combate e navios dos mais avançados, de acordo com o relatório preparado para os líderes do Pentágono pelo Conselho de Ciência da Defesa.

Segundo a mesma fonte, são identificados como comprometidos projetos como o novo caça F/A-18, o V-22 Osprey, o helicóptero Black Hawk e um novo navio de combate litoral, projetado para patrulhar águas perto da costa.

Na lista encontra-se o sistema mais caro de armas jamais construído o F-35 Joint Strike Fighter.

30 Definição de "hacker" - na sua origem refere-se ao hobby/profissão de trabalhar com computadores, evoluindo para a atividade ou ação de invadir, penetrar em sistemas computacionais sem autorização prévia. Importa referir que "hacker" está associado ao ato de "construir coisas " sendo o seu antónimo crackers "destruir as coisas". Tal como é definido pela IBM - Internet Security Systems – acedido em 16 de Fevereiro de 2012. Definição disponível para consulta em:
http://www.iss.net/security_center/advice/Underground/Hacking/default.htm

Figura 5 - F35 Joint Strike Fighter Vs Chengdu J-20 (Jian-20)

(Fonte Imagem – Adaptado da Informação cedida pelo Mr. Matan Efrima, Director de Business Development & Marketing at Verint Communications and Cyber Intelligence Solutions)

Como podemos constatar, a China procura na Guerra de Informação vantagens para modernizar suas forças armadas, estando a investir em formas de superar a vantagem militar de outras potências usando a ciber-espionagem, como ferramenta fundamental para alimentar esse esforço.

Ainda de acordo com o Washington Post, no artigo anteriormente citado, o Pentágono**,** pela primeira vez, citou especificamente o governo chinês e os militares chineses como culpados de invasões no governo e outros sistemas de computador pertencentes aos EUA.

Do ponto de vista estratégico, a guerra de informação pode ser considerada enquanto recurso pela posse de informação. Não sendo necessariamente um fim estratégico, mas uma funcionalidade em torno de um campo de ação estratégica/geoestratégica.

Contudo as ciber-operações não se restringem apenas às chamadas *guerras de informação*. Temos ainda de considerar:

Guerra económica - descrição de ataque e defesa recorrendo a métodos que as empresas enfrentam na competição económica global.

Neste contexto o recurso a *intelligence* e a ciber-espionagem são duas táticas usadas para fomentar a Guerra económica, veja-se o caso da espionagem industrial, "Teremos com eles algumas conversas mais duras do que as que já tivemos", afirmou Barack Obama, numa

recente entrevista[31], lamentando a perda de milhões de dólares por causa da "pilhagem informática" e de segredos industriais.

Guerra eletrónica: terminologia militar, o uso bélico do espetro eletromagnético, a interceção e identificação de emissões eletromagnéticas para alterar os sistemas de comunicações inimigas.

Guerra psicológica: terminologia militar que designa a utilização de meios para influenciar a opinião, sentimentos e comportamentos dos elementos adversos a fim de mudar a sua opinião/atitude no sentido de atingir os seus objetivos militares (Huyg, 2008, p. 39).

Covert cyberwarfare: ciberguerra sustentada por operações cobertas e operações clandestinas, com um esforço continuado não somente de roubo de informação, mas também de disrupção prolongada de infraestruturas económicas, financeiras, sociais, políticas e de defesa e segurança, incluindo ataques visando infraestruturas críticas (não somente aquelas que suportam a Nova Pangeia) com as seguintes vertentes em termos estratégicos e operacionais:

- **Ciber-manobras subversivas** – Técnicas que visam a destabilização e subversão do Estado ou de uma determinada ordem.
- **Amplificação de dinâmicas de guerra assimétrica** - A guerra assimétrica, assim como a guerra irregular, é, devido à sua natureza, a guerra dos fracos contra os fortes, a guerra dos pobres contra os ricos. A guerra irregular e a guerra assimétrica são fundamentalmente guerras de desgaste.
- **Dinâmicas sinergéticas com**: guerra económica, psicológica e eletrónica.
- **Ataques convencionais: incluindo após enfraquecimento prolongado devido a ciberguerra sustentada.**

Será agora pertinente melhor conhecer as ameaças que se originam neste sistema.

2.4. Infraestruturas Críticas Nacionais e a Nova Pangeia

É através da totalidade sistémica formada pela Nova Pangeia que são controlados, geridos e monitorizados diversos recursos e infraestruturas fundamentais: redes de distribuição de água e energia, sistemas financeiros, grande parte dos transportes aéreos, marítimos e terrestres, redes de produção de energia, diversos serviços do Estados como as assinaturas

31 Publicada no Jornal de Notícias (2013). Obama acusa China de apoiar ataques informáticos. Publicado em 03-13. Acedido em 6 de Maio de 2013, disponível para consulta em: http://www.jn.pt/PaginaInicial/Mundo/Interior.aspx?content_id=3105261

eletrónicas, o acesso a serviços públicos, um sem número de ações e operações, que se desmaterializaram para se realizarem neste novo espaço.

Claro que esta situação não se restringe ao âmbito da sociedade civil, também no campo militar a sua utilização se massificou, permitindo quebrar barreiras e colocando ao dispor das Forças Armadas, não só novas capacidades em termos de armamento, mas também impactando e aumentando o seu campo de atuação a este novo teatro de operações que a Nova Pangeia proporciona.

Quando um Unmanned Aerial Vehicle (UAV), ou drone, sobrevoa o Afeganistão numa missão de reconhecimento, transmitindo em tempo real imagens do local onde se encontra, sendo pilotado a centenas ou milhares de quilómetros de distância, ele está a realizar uma missão que utiliza recursos da Nova Pangeia.

A anuência desta realidade implica a mudança de paradigma, com a maior utilização do Ciberespaço e este ocupando um espaço cada vez maior na vida quer dos cidadãos quer do Estado e das empresas**,** a sua importância é reforçada, contudo**,** conforme referido por Loureiro dos Santos (2009, p.302): "ao mesmo tempo que o Ciberespaço se tornou indispensável nas sociedades modernas, ele transformou-se numa das suas maiores vulnerabilidades atuais."

A atualidade é rica em acontecimentos que podem ilustrar a importância desta nova realidade, fenómenos como os já referidos da Primavera Árabe no Egito ou o caso Wikileaks.

Por outro lado a apropriação ilícita de informações relativas a programas de armas sofisticadíssimas, como o caso F-35 Joint Strike Fighter, são exemplos que acontecem um pouco por todo o Globo, e que têm impacto direto na Segurança Nacional dos países onde ocorrem, mas também podem criar e conduzir a consequências a nível regional ou global.

Existem por isso diversos pontos de interceção entre Segurança Nacional e a Nova Pangeia.

Com efeito**,** a aparente facilidade como as fronteiras são transpostas, e a multiplicidade de formas e dispositivos que podem ser utilizados para as transpor criam novos pontos a ter em consideração, que, aliados a uma maior velocidade e capacidade de disseminação da informação e conhecimento tornam, a Nova Pangeia num cenário ideal para a condução de operações da mais variada ordem.

Assim, o Estado deve acompanhar os cidadãos e assegurar também no Ciberespaço a sua segurança.

Verifica-se que praticamente todos os países estão a desenvolver iniciativas nesta área, com o objetivo de desenvolverem capacidades para lidarem com esta situação. Naturalmente que EUA, China, Israel, as Coreias e a Rússia são precursores nesta matéria.

A urgência deste assunto levou inclusivamente a NATO a criar estruturas próprias para lidar com esta matéria**,** caso da Nato Cyber Defence Management Authority/CDMA, para a Cibersegurança, baseando na Estónia um Centro de Excelência para atividades de Segurança no Ciberespaço.

Outro exemplo, ao nível dos Estados**,** é a criação no Pentágono (EUA) de um comando para a Ciberguerra e de uma Agência para a Cibersegurança na Casa Branca. A primeira concebe, prepara, planeia e conduz operações militares no Ciberespaço. A segunda fica com a responsabilidade da conceção, execução de atividades de segurança a nível do Estado.

Estes dois exemplos ilustram a forma séria como Organizações e Estados estão a tratar esta matéria, criando ao mais alto nível nas suas estruturas formas de salvaguardarem os seus interesses e recursos.

Os alicerces do Estado Moderno e a organização na qual estes assentam dependem grandemente de um conjunto de infraestruturas críticas (IC) que asseguram o seu correto e pleno funcionamento.

Num estudo realizado em Portugal, pelo então Conselho Nacional de Planeamento Civil de Emergência, e apresentado em 2007, identificava-se já mais de 150 pontos críticos em cerca de 30 setores estratégicos (Lopes, 2012).

No ordenamento jurídico português, nomeadamente o Dec. Lei n.º 62/2011 Art. 2º de 9 de Maio, define-se infraestruturas críticas nacionais (ICN) como: "uma componente, sistema ou parte de um sistema residente em Portugal que é essencial para a manutenção de funções vitais para a sociedade, saúde, segurança e o bem-estar económico ou social, e cuja conturbação ou destruição impacta ou impossibilita a capacidade para serem asseguradas essas funções". Ainda no mesmo Decreto é apresentada uma definição para infraestrutura crítica europeia (ICE), que no essencial acrescenta**,** a esta definição, o carácter de dependência intersectorial e internacional de uma determinada IC situada no nosso país.

Maioritariamente e de acordo com o referido decreto, são apresentadas como ICE os sectores da Energia e Transportes, contudo e para o presente trabalho, interessa para além destes conhecer e avaliar o impacto de uma eventual disfunção, provocada por Ataques Cibernéticos nas IC contidas num universo mais alargado e diretamente relacionadas com a Nova Pangeia, desta forma recorre-se à classificação das infraestruturas críticas segundo a Homeland Security [32] onde são identificados 16 sectores de IC**,** essa análise é realizada numa reflexão agrupada e organizada por forma a identificar as principais vulnerabilidades e vias de ataque,

32 Nota: Departamento de Segurança Interna dos EUA segundo a Diretiva Presidencial 21 (PPD-21): Segurança Infraestrutura crítica e Resiliência avanços de uma política nacional para fortalecer e manter a segurança, funcionamento e infraestrutura crítica resiliente. Acedido em 18 de Março de 2013. Mais informação disponível para consulta em: http://www.dhs.gov/critical-infrastructure-sectors

avaliando consequências para a Segurança do Estado, sempre numa perspetiva relacionada com a Nova Pangeia.

2.4.1. Energia, Barragens e Nuclear

Grande parte do PIB Mundial encontra-se dependente do sector energético, este sector agrega os segmentos da produção de energia elétrica, petróleo e gás, sendo um sector estratégico, é um dos principais responsáveis por manter a funcionar as sociedades modernas tanto quanto as conhecemos.

Segundo o Departamento de Segurança Interna dos EUA os incidentes/Ciber Ataques relatados pelo sector de energia representaram 53% de todos os incidentes relatados entre Dezembro de 2012 e Maio de 2013**,** o que representou um aumento de 41% face ao semestre anterior (King, 2013).

Embora os segmentos que compõem este sector sejam diferentes, tendo naturalmente diversas especificidades, possuem um conjunto de vulnerabilidades que podem em traços gerais ser consideradas como comuns em termos de Ciber Ameaças.

Por outro lado, trata-se de um sector com muitas interdependências, uma vez que podemos obter energia elétrica usando a transformação de petróleo ou gás, e para obtermos petróleo ou gás, podemos ter que empregar energia elétrica.

Desta forma em termos de Ciber Ameaças podemos seguir o mesmo raciocínio uma vez que as principais vulnerabilidades deste sector se situam ao nível das redes e equipamentos informáticos, que cada vez mais tendem a ser empregues em grande escala para comunicar, gerir, monitorizar e controlar diversos aspetos relacionados com este sector. Da extração à distribuição, essas redes, e esses equipamentos são potenciais pontos de vulnerabilidade para além de se encontrarem dependentes de fontes de energia para garantir o seu funcionamento. Por seu turno**,** são alvos visíveis e de grande dimensão e que cada vez mais dependem da Nova Pangeia, para assegurarem o seu funcionamento.

Podemos adicionar a estas vulnerabilidades**,** na sua grande maioria**,** o facto de as infraestruturas empregues no *core (núcleo)* deste sector terem um ciclo de vida económico longo, diretamente relacionado com a sua natureza e dimensão. Um investimento num Gasoduto, por exemplo, é um investimento que se realiza a longo prazo**.** Assim sendo, a sua obsolescência pode ser também considerada uma vulnerabilidade.

Em termos de Ciber Ataques, podem ser identificadas duas grandes vias: 1ª) diretamente atacando os sistemas através da rede informática que os suporta, sendo o ataque mais comum do tipo *Brute force* (King, 2013)*,* conduzido através da repetição continuada de ataques tentativa/erro, que visam *violar* o sistema de segurança, muitas vezes utilizando ferramentas automatizadas que correm em ciclos e que se destinam a ganhar controlo sobre determinados

sistemas. Ou 2ª) utilizando uma estratégia indireta do tipo Cavalo de Troia, em que antes de se atingir a rede informática, se tenta a penetração através do recurso a um dispositivo, que, após alojado, se transmitirá na rede, contaminando outros dispositivos e sistemas, podendo levar ao seu colapso ou inépcia de parte ou partes da Infraestrutura.

Um exemplo desta estratégia de ataque pode ser o Stuxnet perpetrado numa central nuclear, ao passo que um ataque direto poderia ser realizado, em termos de cenário, a uma barragem, em que através da intrusão na rede de controlo dos sistemas, se forçasse a paragem de fornecimento de energia e abertura das comportas, realizando uma descarga em grande escala.

Neste caso, a severidade desta situação poderia ser proporcional à importância dessa barragem, caso fosse transnacional, poderia inclusivamente afetar mais do que um País, podendo levar ao colapso do sistema e afetar esses Estados ou Estado, criando uma situação de crise.

O potencial de devastação de um ataque deste género pode ser demonstrado quando no dia 17 de Agosto de 2009 perto de Sayanogorsk (Titevski, 2011a) no sul da Rússia, uma das maiores barragens deste país sofreu um acidente. Uma das suas turbinas explodiu, matando 85 pessoas e provocando danos nas restantes 10 turbinas, esta explosão libertou 40 toneladas de óleo no rio Yenisei, causando a morte a cerca de 400 toneladas de peixe, e originando danos de mais de 680 milhões de dólares (Titevski, 2011b). Embora não se trate de um Ciber Ataque, em termos de cenário, recorre-se a este exemplo apenas para ilustrar o potencial de dano.

Podemos ainda considerar uma situação de maior severidade, caso o ataque se realizasse a uma central nuclear, ou fosse realizado com êxito a uma grande refinaria, sendo que os efeitos teriam uma escala de devastação potencial ainda maior, podendo inclusivamente propagarem-se em termos Globais, com o aumento dos preços da energia ou combustíveis. As falhas neste sector podem impactar outros sectores que se encontram dependentes destas fontes, por exemplo o sector dos transportes[33], somado ao impacto que poderia provocar nas populações com situações de desastres ou ausência de energia para a realização de funções básicas.

2.4.2. Transportes

O Sector dos Transportes é o grande responsável pela mobilidade de pessoas e bens, é ele que assegura diariamente, em termos mundiais, muitas das funções vitais. Do transporte de alimentos para as cidades à deslocação de pessoas é um sector de importância estratégia vital. Por outro lado, é um sistema interligado a uma escala Global sendo composto por sete

33 Fonte: Departamento de Segurança Interna dos EUA; "Energy Sector Overview"; mais informação disponível para consulta em: http://www.dhs.gov/energy-sector

segmentos-chave[34]: Aviação, Autoestradas, Transporte Marítimo, Transporte de Passageiros, Transportes de Carga[35], Pipeline, Correios e Serviços Postais.

Grande parte deste sector depende de mecanismos assegurados pela Nova Pangeia para garantir o seu funcionamento. Da monitorização de tráfego nas autoestradas à sinalização das linhas férreas, passando pelo controlo de tráfego aéreo e portuário à vigilância de linhas e autoestradas, a comunicação eletrónica e distribuição inteligente de correio, todas estas funções se intercetam com a Nova Pangeia.

Muitas das tecnologias que estão na base do suporte a este sector em termos de gestão, monitorização e controlo, recorrem a protocolos SCADA [36] comummente utilizados em diversas áreas. Por outro lado, tem-se vindo a assistir a uma substituição de sistemas desenvolvidos por medida e na sua grande maioria proprietários e fechados, por sistemas do tipo COTS[37] mais abertos e acessíveis em geral (Abraham & Goodman 2001, pag. 74).

Esta alteração de paradigma, a cada vez maior necessidade de comunicação entre sistemas centrais e remotos/distribuídos trouxe algumas vulnerabilidades que se podem somar à grande visibilidade deste sector, sendo o seu colapso ou afetação rapidamente percecionados e os seus efeitos rapidamente visíveis.

Existe claramente potencial para indivíduos/organizações com motivações políticas, religiosas ou criminosas fazerem uso de ferramentas tecnológicas para abusar, adulterar, adquirir controlo ou corromper sistemas e por essa via causarem danos assinaláveis (Abraham & Goodman 2001, pag. 74).

Veja-se o caso dos atentados de 11 de março de 2004 em Madrid[38]. Um Ciber Ataque**,** visando uma rede de controlo ferroviário, poderia produzir também efeitos devastadores, bastaria para isso que conseguisse adquirir controlo remoto sobre as agulhas de uma ferrovia através

34 Nota: Segundo o Departamento de Segurança Interna dos EUA segundo, mais informação disponível para consulta em: http://www.dhs.gov/transportation-systems-sector

35 Nota: Inclui Transporte Ferroviário e Rodoviário

36 Nota: Supervisory Control and Data Acquisition - atualmente assegura a grande maioria de interfaces de linguagem de comando, entre Homem-Máquina, sendo um exemplo bastante comum a mudança de sinalização remota numa linha de ferrovia ou a abertura de uma determinada porta numa fábrica, dá-se um comando num sistema central ou periférico, que será transmitido na rede, e que, por ação desse protocolo, chega a um determinado equipamento, que recebe a instrução e provoca uma ação ou ações, do ponto de vista físico e móvel, tendo efeitos para além do seu domínio e produzindo interações com outro tipo de sistemas ou funções ultrapassando dessa forma o seu domínio e influindo noutros domínios e sistemas, para além da sua origem ou fronteira.

37 Nota: Commercial-Off-The-Shelf

38 Nota: Neste ataque dez bombas explodiram em quarto comboios que faziam a ligação entre Alcalá de Henares e a estação madrilena de Atocha, 191 pessoas morreram e milhares ficaram feridas, as imagens deste ultrajante ataque correram o mundo.

da infiltração na rede de comunicações de um operador ferroviário, para se conseguir conduzir um comboio, numa trajetória de colisão e com isso produzir danos assinaláveis.

A mesma filosofia**,** em termos de impacto e tipo de ataque, pode ser invocada para os restantes segmentos, caso se consiga alcançar na rede os pontos de controlo, sem exceção o ataque e a produção de dano fica facilitada.

Atente-se ao exemplo do controlo de tráfego aéreo ou de tráfego portuário, se através da Nova Pangeia se conseguir afetar, trocar ou falsear mensagens trocadas entre um centro de controlo e um navio ou avião, a rota destes podia ser alterada provocando intencionalmente acidentes.

Em 2013 na "Defcon Hacking Conference" em Las Vegas, um consultor informático, Brad Haines, conhecido on-line por "RenderMan", demonstrou como se podiam explorar, por *spoofing*[39]**,** os sistemas de sinalização na aviação comercial que servem para emissão de sinais de rádio que marcam a identidade e localização das aeronaves nos radares[40], a falta de encriptação e autenticação destes sistemas permitiria, segundo a demonstração, injetar inúmeros sinais/aviões fantasmas num radar de controlo de tráfego aéreo, lançando a confusão e impedindo ao controlador a correta gestão da situação (Armerding, 2013).

Numa outra conferência "Hack in the Box" também em 2013, em Amesterdão, um consultor alemão**,** Hugo Teso, demonstrou na sua apresentação "Aircraft Hacking"[41], como atacar remotamente e tomar o controlo total de uma aeronave. Através da exploração de uma falha do sistema ACARS, sistema que permite em tempo real a comunicação entre os sistemas da aeronave e os aeroportos e sistemas de controlo, seria capaz de invadir o computador de bordo do avião, usando uma aplicação PlaneSploit a correr no seu telemóvel (Storm, 2013), conquistando**,** desta forma**,** controlo do sistema e fazendo *upload* de informações de voo FMS. Uma vez no computador de bordo do avião, torna-se possível manipular a rota da aeronave de forma automática, dado que muitos dos aviões modernos já não dispõem de controlos analógicos, o avião fica totalmente à mercê do Hacker.

As técnicas apresentadas podiam muito bem ser empregues para criar um acidente de grandes dimensões numa ou em diversas cidades, criando uma situação de desastre potencialmente grave, não só pela morte de passageiros a bordo mas também pelos alvos que essas aeronaves podiam atingir com o seu impacto, trata-se assim de um cenário de grande severidade para o Estado.

39 Nota: IP spoofing, ou apenas spoofing é uma técnica de ataque que consiste em esconder/mascarar pacotes IP utilizando endereços de remetentes que são falsos ou falsificados.
40 Nota: Sistemas do tipo NextGen - ADS-B Automatic Dependent Surveillance-Broadcast.
41Nota: Acedida em 17 de Fevereiro de 2014. Apresentação disponível para consulta em:http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf

O mesmo se podia extrapolar para um sistema de controlo de semáforos numa via ou estrada, caso não exista sincronização na sinalização podem ser causados acidentes, razões pelas quais alguns países como a Coreia do Sul estão a avançar para construções de centros de informação de tráfego, que usam já sistemas e ferramentas que visam a proteção contra Ciber Ataques (Yonhap, 2011).

Nestes casos as principais vias de ataque podem-se situar na intrusão na rede, para aquisição e controlo de sistemas ou junto dos sistemas em si, usando outros mecanismos, como os suportes físicos[42] para disseminar o ataque.

Naturalmente que a severidade dos ataques para o Estado varia sendo o espectro de efeitos bastante alargado, contudo**,** em qualquer um dos segmentos assinalados**,** esses ataques podem produzir efeitos de monta.

Da escassez de matérias-primas fundamentais e alimentos, por exemplo no Reino Unido 95% das frutas e 50% dos vegetais consumidos são importados (Giurgiu, 2013)**,** num cenário de intrusão ou disrupção de sistema de transporte ou parte dele podem-se causar distúrbios a longo prazo, como a subida de preços por efeito da interrupção de Portos, Aeroportos e Ferrovias motivados por Ciber Ataques, ataques que prolongadamente impeçam o normal fornecimento das cadeias de distribuição, levando a uma escassez ou ao encerramento de meios como medida de segurança**,** ou mesmo pela produção de danos, caso se conseguisse "comandar" um avião para um alvo logístico e com a sua queda produzir danos na cadeia de distribuição.

Este tipo de cenário pode também contribuir para a lassidão do Estado, quer pela perca ou afetação de cadeias de logística e distribuição, quer pela perca de vias essenciais de comunicação, afetando ainda a mobilidade e capacidade de resposta, por exemplo com Ciber Ataques produzidos com êxito aos sistemas de controlo de vias de comunicação principais como as autoestradas ou sistemas de controlo de trânsito em grandes cidades, risco real e para o qual**,** como já assinalado, existem iniciativas para os mitigarem.

A possibilidade de serem produzidos Ciber Ataques a outras IC, por exemplo situadas no sector energético, e estes produzirem colateralmente efeitos combinados afetando também este sector, é um cenário que se pode colocar.

Um analista Senior da CIA, Tom Donahue, afirmou numa conferência do SANS Institute em New Orleans (Espiner, 2008), que foram registados diversos ataques cibernéticos contra infraestruturas do sector energético, afetando várias regiões, sendo que pelo menos um causou uma quebra de energia em várias cidades.

42 Nota: Dispositivos do tipo Pen Usb ou discos rígidos

Ora esta situação de *blackout,* muito embora grande parte das IC de ambos os sectores possuam sistemas de redundância e continuidade de serviço, quando escalada a várias cidades e por tempo indeterminado, pode causar situações de fraqueza e vulnerabilidade, por exemplo nos transportes ferroviários e redes de metro, no controlo de trânsito ou tráfego aéreo e portuário, não só pela falta de energia que conduz à inoperacionalidade dos sistemas, mas também pela ausência em operação da plenitude das IC**,** o que pode ser aproveitado num Ciber Ataque, uma vez que normalmente os sistemas ficam diminuídos ao trabalharem abaixo da sua capacidade, para ampliar um ataque ou desferir um golpe que mais facilmente produza efeitos.

2.4.3. Financeiro

A economia mundial encontra-se dependente do sector Financeiro e dos serviços globais que este assegura. Cidadãos, Empresas, Instituições e o próprio Estado, todos recorrem e dependem de um conjunto alargado de transações e serviços que na sua grande maioria são realizados e assegurados na Nova Pangeia.

Estes serviços permitem[43]:

- Depósito de fundos e pagamentos;
- Providência de crédito e liquidez a clientes;
- Investimento em fundos ou instrumentos financeiros de longo e curto prazo;
- Aceitam riscos financeiros;
- Transferências entre clientes.

Este conjunto básico de serviços representa a grande maioria das operações realizadas neste sector, tem a particularidade de poder ser realizado a uma escala Global, e por múltiplas formas, por transferência eletrónica, através de um computador ou dispositivo móvel.

Estima-se que apenas no Reino Unido em 2012, o segmento de compras on-line tenha realizado 77 biliões de Libras em transações (IMRG Capgemini, 2012). Com este número podemos perspetivar a ordem de grandeza e a importância que este sector desempenha no contexto da sociedade atual.

Naturalmente que esta realidade implica que este sector se tenha tornado bastante apetecível e mais exposto a Ataques Cibernéticos, os quais são cada vez mais frequentes e sofisticados.

Estes ataques ocorrem de forma direta ou indireta. Indiretamente, através de *phishing*, em que os dados ou informações são obtidos por intermédio de esquemas de camuflagem, tipicamente é solicitado ao cliente final a resposta a informação por intermédio de veículos falsos, que chegam ao cliente através de email, mensagem curta ou internet, sendo que o

43 Fonte: Segundo o Departamento de Segurança Interna dos EUA, mais informação disponível para consulta em: http://www.dhs.gov/financial-services-sector

utilizador final pensa que está a responder à sua instituição, mas na realidade está a responder a uma terceira entidade, que depois irá usar os seus dados para operações ilícitas, transferências, pagamentos indevidos ou desvios.

De acordo com uma pesquisa realizada pela Gartner Inc (Stamford, 2007), só nos EUA em 2007, foram perdidos 3,2 biliões de dólares com este tipo de ataques, sendo que foram afetadas mais de 3,6 milhões de pessoas.

Os ataques de tipo indireto podem assumir diversas formas como o conhecido Projeto Blitzkrieg (Price Waterhouse Coopers, 2013), através da proliferação de um software malicioso, *malware*, que**,** hospedado num computador**,** para além de se espalhar em rede, recolhe dados relativos a operações financeiras, regista esses dados e envia para terceiros, que os usam indevidamente, prevê-se que o grupo relacionado com este projeto tenha realizado com este esquema 5 milhões de dólares em roubos.

Contudo as ameaças também se registam de forma direta na rede, tipicamente tratam-se de ataques do tipo DoS que se destinam a causar perturbações ou falhas de serviço, tentando colapsar os sistemas.

Este tipo de ataque tem evoluído para ataques do tipo "brute-force" que tentam incessantemente obter respostas dos sistemas, através de processos automáticos de tentativa e erro, por exemplo preenchendo nomes de utilizadores e *passwords* aleatórias até serem encontradas respostas verdadeiras que permitam descobrir falhas e assim entrar no sistema e realizar operações não autorizadas.

Segundo a PWC, enquanto os ataques DoS anteriores contra instituições financeiras provinham maioritariamente de *hacktivists* como os Anonymous/Occupy Wall Street, surgem receios de ataques DoS lançados por Estados, suspeitando-se que o governo Iraniano tenha recorrido a este tipo de ataque, configurando uma situação de State Sponsored Attack, e escalando este tipo de ameaças a outro nível, uma vez que o tipo e número de recursos envolvidos são substancialmente maiores.

Ainda segundo a PWC, o Cibercrime em termos Globais, aumentou em 2012 sendo responsável por 38% da criminalidade económica neste sector, em comparação com 16% em outros sectores (Ashford, 2012).

O aumentar de incidentes reportados neste sector denuncia o nível de ameaça a que se encontra exposto, sendo um sector hiperconectado, global e onde se registam milhões de transações por segundo**,** podemos antecipar desde logo, as consequências de uma situação de impedimento ou colapso dos serviços prestados.

Se tivermos em consideração que os 10 maiores detentores de reservas internacionais respondem por quase dois terços do total de reservas em moeda estrangeira do mundo

(Pasquali, 2012), podemos inferir sobre múltiplos cenários e suas consequências para os Estados e sua segurança. Caso se registe um incidente grave, o impedimento de operações simples como o contacto com a Banca, a situações mais delicadas como as transações falsas a larga escala, ou movimentos fictícios de divisas, poderiam gerar crises nacionais, transnacionais ou até mesmo globais, podendo colocar em causa o equilíbrio do sistema financeiro mundial, caso um ataque em larga escala tivesse efeito em diversos alvos de forma combinada, poderia gerar o colapso e a desordem global levando ao caos financeiro e económico, gerando também efeitos colaterais noutros sectores que se encontram dependentes do financeiro.

2.4.4. Governo e Defesa, Emergência e Saúde

A dependência sistémica destes sectores favorece uma análise conjunta em termos de IC, sendo sectores onde a Nova Pangeia cresce de importância desempenhando um papel chave.

As formas de governação na Nova Pangeia cativam cada vez mais adeptos, o chamado eGovernment é inclusivamente alvo de *Benchmark* anual e engloba para além dos 28 Estados-Membros da União Europeia, a Islândia, a Suíça e a Turquia[44].

Na edição de 2012 deste *Benchmark,* foram avaliados três eventos de vida: "Iniciar uma Empresa e Primeiras Operações", "Perder e Encontrar um Emprego" e "Estudar"[45]. Estas 3 ocasiões quotidianas, outrora requerendo um contacto físico e material, são agora alvo de avaliação e distinção para aqueles países onde a sua realização na Nova Pangeia mais acessivelmente, facilmente e desmaterializadamente se realiza.

Este novo paradigma estende-se a outras vertentes da Governação e do Estado, tendo a Europa um lugar cimeiro na adoção destas novas práticas, impulso esse, que decididamente se dá com a Estratégia de Lisboa que visa transformar a Europa "na economia do conhecimento mais competitiva e dinâmica do mundo, capaz de um crescimento económico sustentável, acompanhado da melhoria quantitativa e qualitativa do emprego e de maior coesão social"[46].

Ora esta visão Europeia é uma visão onde a Nova Pangeia assume uma dimensão preponderante, funcionando como pilar e como fonte de dinamização social e económica.

Também no sector da Defesa a Nova Pangeia se afirma, para além dos exemplos já citados, da Geórgia ou no caso das operações remotas com UAV encontrou-se uma nova forma de fazer Guerra que recorre extensivamente ao uso deste novo espaço estratégico.

44 Fonte: European e-Government Benchmark, promovido pela comissão europeia.
45 Fonte: Idem
46Para mais informações acerca da estratégia de Lisboa consultar:
http://ec.europa.eu/growthandjobs/index_en.htm

Se**,** por outro lado, estabelecermos uma ligação aos sectores de Emergência e Saúde[47], que normalmente compreendem as áreas de Forças de Segurança, Bombeiros e Serviços de Emergência, Proteção Civil, Serviços Médicos de Emergência, Serviços Públicos de Saúde e Privados, podemos encontrar pontos de interseção e um denominador comum, as redes avançadas de comunicações que, numa primeira instância naturalmente estabelecem ligações e servem para comunicar, mas que de uma forma mais lata e dentro do contexto da Nova Pangeia, ligam sistemas. Recorrendo ao exemplo de um grande incêndio, ou uma operação de emergência em situação de catástrofe, torna-se necessário a coordenação de meios e recursos diversos, onde a localização destes é fundamental, o acesso a informação em tempo real e a sistemas de informação precisos torna-se uma vantagem estratégica e tática.

Exemplo disso é o forte investimento que alguns fabricantes mundiais de Tecnologias de Informação estão a realizar nesta área. A IBM, por debaixo de um "chapéu" que apelida de Cidades Inteligentes (IBM Institute for Business Value, 2013) apresenta soluções que podem consolidar e abarcar todos estes sectores. Da informação de trânsito em tempo real recolhida por sensores, a informação sobre um determinado acidente, que através da localização da ocorrência decide qual o meio de socorro mais próximo, se existe necessidade de envolver forças de segurança ou corpos de bombeiros, que rota deve seguir, que profissionais de emergência tem a bordo, e que competências têm para responder a esse tipo de situação, que instalação de emergência está mais próxima, qual a sua disponibilidade e recursos para atender.

Estas**,** entre muitas outras perguntas, podem encontrar a resposta de forma integrada num sistema como o que a IBM propõe, embora possa parecer uma visão bastante holística e futurista, ela segundo a IBM é possível hoje, mas apenas é possível porque utiliza extensivamente a Nova Pangeia.

Estamos portanto, perante a criação e utilização de um espaço novo, um *Backbone,* que abarca múltiplas dimensões e atividades e se materializa na Nova Pangeia, pelo que a sua disrupção ou colapso pode criar cenários de devastação, por procurarmos cada vez mais respostas neste novo território agudizamos a nossa dependência em relação a ele. Naturalmente que estes sectores podem dispor de respostas convencionais também eficazes, contudo a dependência tecnológica é assinalável.

47 Fonte: Departamento de Segurança Interna dos EUA; "Emergency Sector Services"; e "Healthcare and Public Health Sector" mais informação disponível para consulta em : http://www.dhs.gov/emergency-services-sector e http://www.dhs.gov/healthcare-and-public-health-sector respetivamente

2.4.5. Industrial, Químico e Instalações Comerciais

Os sectores[48] Industriais que abrangem, a fabricação e transformação de metal[49] a fabricação de máquinas[50], equipamento de transporte[51], o Sector Químico[52] e o Sector de Instalações Comerciais[53]. Apresentam-se agrupados numa lógica de "*facilities*", instalações, pelo que desta forma apresentam um denominador comum principal com a Nova Pangeia, o protocolo SCADA[54].

Segundo a tabela[55], "Guide SCADA and SME draft", é apresentada uma lista de ameaças a estas IC, descritas e apresentadas como sendo comuns a todas, são elas:

- **Bot-network operators[56];**
- **Grupos Criminosos[57];**
- **Serviços de Inteligência Nacionais[58];**
- **Hackers[59];**

48 Fonte: Departamento de Segurança Interna dos EUA; "Critical Manufacturing Sector"; "Chemical Sector"; "Commercial Facilities Sector". Acedida em 6 de Abril de 2014.Mais informação disponível para consulta em : http://www.dhs.gov/critical-manufacturing-sector http://www.dhs.gov/chemical-sector
; http://www.dhs.gov/commercial-facilities-sector e respetivamente

49 Nota: incluindo: ferro, aço e ligas leves, alumínio e metais não ferrosos.

50 Nota: incluindo: motores, turbinas, equipamentos de transmissão de energia, equipamento elétrico, eletrodoméstico, e componentes elétricos.

51 Nota: incluindo: Veículos, Aviação e Aeroespacial, Material Circulante.

52 Nota: incluindo: produtos químicos de base, produtos químicos especiais, produtos químicos agrícolas, farmacêutica e produtos de consumo.

53 Nota: incluindo: espaços: públicos de espetáculos, diversão, jogo, hotelaria, eventos e retalho.

54 Nota. SCADA (supervisory control and data acquisition) sistemas/softwares utilizados para comunicar, monitorizar e controlar dispositivos ou sistemas, máquina-máquina ou Homem-máquina.

55 Fonte: Government Accountability Office (GAO), Department of Homeland Security's (DHS's) Role in Critical Infrastructure Protection (CIP) Cybersecurity, GAO-05-434 (Washington, D.C.: May, 2005). Acedida em 13 de Março de 2913.Mais informação disponível em: http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

56 Nota: Bot-network operators – Redes de Hackers, no entanto, em vez de invadirem os sistemas, o seu objetivo principal é garantirem o seu controle, agrupando em conjuntos sistemas violados, e neles executando instruções remotas em massa, programando ataques conjuntos, que inclusivamente podem ser vendidos a terceiros.

57 Nota: Grupos Criminosos - procuram atacar sistemas para ganho monetário. Usam ataques de spam, phishing e spyware/malware para tentarem realizar roubos de identidade e fraude on-line. Normalmente para desencadearem ações de espionagem industrial e depois venderem essas informações também a terceiros.

58 Nota: Serviços de Inteligência Nacionais – Normalmente usam ferramentas para reunirem informações de espionagem. Além disso, vários países estão a trabalhar agressivamente para desenvolver doutrinas no campo da guerra de informação. Esses recursos permitem que uma única entidade tenha a capacidade de perpetrar um ataque com um impacto significativo e sério, como são os casos dos já citados State Sponsored Attacks.

59 Nota: Hackers – Invadem redes ou sistemas com propósitos diversos. Podem estar ativamente envolvidos em atos de hacktivism, ou procurarem o lucro pelo roubo de informação, ou simplesmente procurarem a disrupção quer por desafio, ganho financeiro ou desejo de reconhecimento. Realizam ataques de forma isolada ou organizada em Grupos/Gangues, podendo também incorporar, agências secretas ou outro tipo de organização podendo desencadear o mais variado tipo de ataques, como cyber-black-ops, por exemplo.

- **Insiders [60];**
- **Phishers [61];**
- **Spammers[62]**;
- **Spyware & Malware[63];**
- **Terroristas [64].**

Naturalmente que o grau de ameaça e respetiva severidade é diferente nestes sectores, contudo o tipo de técnicas é transversal. Exemplo disso foi o ataque denominado como "Nitro" (Prince, 2011). Segundo a Symantec o ataque terá sido inicialmente dirigido a organizações de direitos humanos passando mais tarde para a indústria automóvel, alastrando-se à indústria química, atingindo só nesse sector 29 empresas nos EUA, tendo no total atingindo pelo menos 48 empresas das 100 que constituem o ranking da Fortune.

Os ataques foram executados por estágios, com o conhecido PoisonIvy Trojan, disseminado por e-mail. Uma vez no sistema, o *malware* abriria uma *backdoor*, comunicando com um servidor remoto e fornecendo o mapa da rede, e através dele, iniciar-se-ia o acesso aos sistemas internos, expondo assim para o exterior os sistemas e a sua informação.

Estes quando ganham acesso aos sistemas podem causar danos consideráveis, quer por poderem revelar informações secretas de índole industrial, plantas secretas de edifícios ou por poderem destruir sistemas e enviar instruções remotas, que podem produzir danos nas instalações industriais ou colateralmente nas populações.

60 Nota: Insiders – Um insider (pessoa pertencente à organização) que esteja descontente é a principal fonte de criminalidade informática. Estes podem não precisar de uma grande quantidade de conhecimentos sobre o sistemas, porque o seu conhecimento da organização interna e as suas permissões, muitas vezes conferem-lhe acesso irrestrito, podendo desta forma causar danos nos sistemas ou até roubarem/extraírem informações deles. A ameaça interna pode também incluir fornecedores, por exemplo de outsourcing, bem como funcionários que acidentalmente introduzem malware nos sistemas, por negligência.

61 Nota: Phishers - Indivíduos ou grupos, que executam esquemas de phishing, tentativa de roubo de identidade, dados ou informações falseando dando ao utilizador final a ideia de que está a lidar com um sistema verdadeiro, quando este, é apenas uma fachada para a recolha de informação e posterior uso indevido.

62 Nota: Spammers – Indivíduos ou organizações que distribuem e-mails indesejados com informações ocultas ou falsas, por forma a venderem produtos ou distribuir spyware /malware. Podem causar nestes sectores, o colapso dos sistemas, por os sobrecarregarem com informação ou pedidos em excesso, criando uma situação de DoS.

63 Nota: Spyware & Malware – Distribuição de código ou aplicações malignas, com o objetivo de recolher informação ou causar danos no sistema pela sua infeção criando situações de mau funcionamento que podem provocar paragens no sistema, por exemplo, pela execução de instruções erradas.

64 Nota: Terroristas – Procuram destruir, incapacitar, ou explorar as infraestruturas críticas, a fim de causar ameaças à segurança nacional, causar mortes em massa, enfraquecer a economia, e danificar a moral pública e a sua confiança, são objetivos frequentes. Os terroristas podem usar esquemas e técnicas combinadas, como as anteriormente descritas, para provocarem danos. Por exemplo, pondere-se um ataque a uma Instalação industrial de Química Pesada, onde com êxito sejam adquiridos os comandos dos sistemas de produção ou mistura de componentes, o seu mau funcionamento poderia levar a situações potencialmente perigosas quer para a instalação industrial em si quer para as populações circundantes.

2.4.6. Alimentação, Agricultura e Água

Segundo a FAD - Food and Drug Administration nos EUA[65] no seu relatório para a Agricultura e Alimentação, parte do Plano Setorial Específico de Proteção de Infraestruturas Criticas Nacionais, de 2010, refere-se que os Ciber Ataques a estes sectores oferecem pouco ganho financeiro, representando apenas uma perturbação económica mínima, pelo que não se reconheciam neles alvos preferenciais ou usuais, não os assumindo como ameaças prioritárias.

Contudo isso não invalida que estejam totalmente a salvo de ataques provenientes da Nova Pangeia. Uma vez que recorrem ao uso de protocolos SCADA, estão expostos. Embora comparativamente com as outras IC já analisadas o grau de dependência e interceção com a Nova Pangeia é reduzido, mais ainda assim existe.

Por exemplo a indústrias de produção alimentar empregam extensivamente tecnologias nas suas cadeias de produção, recorrendo a sistemas e redes informáticas para os controlar.

Caso esses processos sejam interrompidos, grande parte do resultado do ataque ficará confinado a esse espaço, sendo baixa a sua capacidade de afetar outros campos ou atividades relacionadas, contudo podem ser atacados.

De igual forma no Sector Agrícola, o seu potencial de devastação será reduzido. Muito embora a chamada agricultura de precisão[66] comece a ser mais praticada, grande parte das suas funcionalidades, reside na monitorização das explorações e na recolha de indicadores que possibilitem uma tomada de decisão mais avisada em termos da gestão da exploração. Se estas funcionalidades se alargarem, substituindo cada vez mais a intervenção humana, as ameaças aumentarão. Exemplo disso será a gestão de sistemas de rega ou aplicação de adubos em modo automático. Caso atacados, podem produzir efeitos negativos, para a produção e exploração, pois esta poderia ficar contaminada por excesso de adubos.

No entanto no Sector da Água, nomeadamente na área da distribuição e armazenamento de água potável, existem inúmeros incidentes que dão conta de ataques ou tentativas de ataques.

65 Fonte: FAD - Food and Agriculture Sector-Specific Plan - An Annex to the National Infrastructure Protection Plan. Acedida em 6 de Abril de 2014. Mais informação disponível para consulta em: http://www.fda.gov/downloads/Food/FoodDefense/UCM243043.pdf

66 Definição: modelo de agricultura que adota tecnologias de informação e comunicação tão distintas como: Sistemas de Informação Geográfica (SIG), Sistemas de Posicionamento Global (GPS), Deteção Remota, Tecnologias de Débito Variável (VRT), Sensores diversos, Telecomunicações, Sistemas de apoio à decisão, etc. A Agricultura de Precisão aparece, geralmente, com dois objetivos genéricos: o aumento do rendimento dos agricultores; e, a redução do impacte ambiental resultante da atividade agrícola. Fonte: AJAP - Associação dos Jovens Agricultores de Portugal. Acedida em 12 de Abril de 2014. Mais informação disponível para consulta em: http://agrinov.ajap.pt/agriprecisao.asp

Segundo a Reuters (Finkle, 2011) nos EUA foi publicado um relatório, onde um alegado grupo de Hackers conseguiu desligar remotamente a bomba de água de um ponto de exploração no centro de Illinois. Segundo esta fonte, terá inclusivamente sido o primeiro Ciber Ataque, conhecido e perpetrado por estrangeiros a um sistema industrial dos EUA.

Os atacantes terão ganho acesso à rede de serviços públicos de água a partir de uma comunidade rural a oeste da capital do estado de Springfield. Com as credenciais roubadas, ganharam acesso e privilégios para controlar sistemas industriais nessa rede, segundo o relatório, provocando inclusivamente a paragem de sistemas.

Noutro incidente, reportado por um alto funcionário do Estado Israelita, Prof. Yitzhak Ben Yisrael,[67] uma divisão do Exército Eletrónico Sírio terá tentado atacar os sistemas de água da cidade de Haifa, ataque esse que não surtiu efeito por ter sido bloqueado atempadamente, tendo sido realizado por retaliação a bombardeamentos efetuados pelas Forças Armadas de Israel a alvos no território Sírio.

Neste caso, temos uma situação clara, em que o espaço de batalha convencional é levado para a Nova Pangeia, mostrando uma interligação cada vez mais próxima entre campos de batalha e demonstrando o uso pleno deste novo território como um campo fértil para o desenvolvimento de ações de guerra ou guerrilha.

Embora não tenham sido apresentados os efeitos, estas situações ilustram o seu potencial, e colocam sobre este setor uma pressão adicional.

2.4.7. TIC - Tecnologias da Informação e Comunicação

Sendo um ponto central da Nova Pangeia, o seu estudo tem-se desenvolvido ao longo deste trabalho, sendo que em termos de ameaças a sua análise será realizada em larga medida, no Ponto 3.2 - Análise de Ameaças às infraestruturas da Nova Pangeia, recorrendo a teias mórficas[68] para a elaboração de cenários de ameaça.

Interessa porém realçar a importância deste sector como fundamental, não fossem os avançados sistemas de informação e os diversos componentes tecnológicos que o compõem, tornando possível o seu funcionamento, ligação e interação com outros sistemas e utilizadores, e a Nova Pangeia ficaria vazia, não fazendo sentido a sua análise.

67 Nota: Presidente do Concelho Nacional de Investigação e Desenvolvimento do Ministério das Ciências Israelitas citado por Ronen, Gil; "Syrian Cyber-Attack on Haifa Water System"; Israel National News; Maio de 2011. Acedida em 6 de Abril de 2014. Mais Informação disponível para consulta em: http://www.israelnationalnews.com/News/News.aspx/168306#.UqcHztTuP4g

68 Nota: Formação de ligações, morfismos, que permitam identificar ameaças e avaliar, mediante a construção de cenários, o impacto e risco que estas fontes representam para o sistema, tentando inferir do seu potencial de colapso.

Segundo o Departamento de Segurança Interna dos EUA [69] estes sectores (TIC) são fundamentais para a segurança dos Estados, economia, saúde pública, empresas, governos, universidades e cidadãos privados. São assim ativos estratégicos com intersecção aos mais variados níveis e nos mais variados sectores.

Inclusivamente o seu eixo de influência prolonga-se para o exterior do Planeta, alongando-se ao espaço sideral através de satélites e outro tipo de veículos que dependem de comunicações e sistemas de informação.

Interessa avaliar se existem vulnerabilidades ou ameaças a este nível, uma vez que os satélites também desempenham um papel fulcral, assegurando comunicações e transmissões globais, funcionando como sistemas de alerta, meteorologia, navegação, reconhecimento, controlo remoto e vigilância (Paganini, 2013).

Desta forma os serviços prestados por satélites cobrem praticamente todos os sectores de atividade pela sua importância e dependência, podendo ser alvos privilegiados e a considerar em possíveis Ciber Ataques (Paganini, 2013).

Segundo a Information Age magazine [70], a US-China Economic and Security Review Commission terá divulgado que supostos Hackers, que se acredita estivessem a operar a partir da China, terão conseguido**,** em 2008, interferir em dois satélites do governo dos EUA, tomando controlo do satélite Landsat-7 por duas vezes durante 11 minutos e acedendo ao Terra AM-1. Embora tenha sido divulgado que os satélites não foram danificados, não foram ventiladas informações sobre o impacto dos ataques.

Contudo, de acordo com a InfoSec Institute (Paganini, 2013), podem ser identificadas 10 ameaças principais nesta vertente:

- **Localização[71]**;
- **Escuta[72]**;
- **Interação[73]**;
- **Uso[74]**

69 Fonte: Departamento de Segurança Interna dos EUA; "Information Technology Sector"; e "Communications Sector" Acedida em 6 de Abril de 2014. Informação disponível para consulta em: http://www.dhs.gov/information-technology-sector e http://www.dhs.gov/communications-sector respetivamente.

70 Fonte: Information Age (2012) - Can satellites be hacked?. Information Age magazine. 29 de Maio. Acedida em 7 de Abril de 2014. Informação disponível para consulta em: http://www.information-age.com/technology/security/2105738/can-satellites-be-hacked

71 Nota: Localização – de ativos ou de informações e dados na Internet e em software;

72 Nota: Escuta – de comunicações e localizações;

73 Nota: Interação – com protocolos de autenticação usados para transmissão de radio e TV;

74 Nota: Uso – tomada de controlo sobre o equipamento para explorar as suas capacidades indevidamente (Transmissão de música, rádio ou outro tipo de conteúdo não oficial)

- **Scanning/attacking**[75];
- **Breaking**[76]**;**
- **Jamming**[77]**;**
- **Mispositioning/Control**[78];
- **Grilling**[79]*;*
- **Collisioning**[80]**.**

O sucesso de um ataque da natureza dos anteriormente descritos pode provocar elevados danos e até levar à perda de vidas humanas. Se tivermos em conta a dependência de sistemas como os de navegação na indústria aeronáutica e automóvel ou sistemas de precisão, como os usados na construção civil, podemos rapidamente entender a necessidade e criticidade na defesa a estes sistemas, que do ponto de vista convencional seriam muito mais difíceis de atingir e**,** através da Nova Pangeia, encontram-se mais expostos e mais acessíveis, por um investimento muitíssimo inferior, em relação aos ataques convencionais.

Por outro lado, em termos de TIC, interessa realçar a importância das redes móveis e da mobilidade, uma vez que são contributos fundamentais para o alargamento da Nova Pangeia.

De acordo com a Internet World Stats (2014), o número de telefones móveis no mundo, no início de 2013, situava-se nos 6,8 biliões cada vez mais próximos dos 7,1 biliões da população mundial.

Com o crescimento da capacidade de processamento e armazenamento nos telefones móveis, e com o advento dos Smartphones, cada vez mais estes dispostitos se assemelham a computadores, estando expostos ao mesmo tipo de ameaças que os anteriores e tendo eles próprios as mesmas capacidades em termos de produção de ameaças, com a particularidade de estarem em mobilidade e poderem lançar ou receber ataques independentemente da sua localização, bastando para isso terem ligação em rede. Interessa pois considerá-los na ótica da Nova Pangeia como mais um elemento das TIC que merece destaque pela sua proliferação e dupla capacidade de representar uma ameaça e ser ao mesmo tempo um alvo a atingir.

75 Nota: Scanning/attacking – uso para ataques anónimos de scanning, DoS, e spoofing;
76 Nota: Breaking – quebra de protocolos de tecnologias mais antigas tipo X.25 para uso indevido;
77 Nota: Jamming – impedir o uso de determinadas frequências, bloqueando ou parando as comunicações;
78 Nota: Mispositioning/Control – controlo e passagem de informação e coordenadas erradas;
79 Nota: Grilling – ativação de todos os painéis solares do satélite, criando uma sobrecarga de energia no sistema e o seu possível dano ou inoperação;
80 Nota: Collisioning – passagem de coordenadas erradas ou falsas, por forma a originar colisões ou do satélite em si, ou de outros sistemas que deste dependam para seu uso/orientação (ex: sistemas GPS).

3. CAPÍTULO - AMEAÇAS VINDAS DO CIBERESPAÇO

Neste Capítulo são explanadas as noções de Segurança e Risco, sendo realizada uma análise "SWOT" e uma análise de Ameaças às infraestruturas da Nova Pangeia, recorrendo-se ao uso de uma teia mórfica para a cenarização e avaliação de fontes de risco e ameaças às infraestruturas da Nova Pangeia.

Interessa pois antes de avançarmos para a noção de risco, revermos dois conceitos relacionados, Ameaça e Segurança.

Podemos considerar **ameaça** como - qualquer acontecimento ou ação (em curso ou previsível), de variada natureza (militar, económica, ambiental, etc.) que contraria a consecução de um objetivo e, que normalmente é causadora de danos, materiais ou morais, sendo que, no âmbito da estratégia, se consideram principalmente as ameaças provenientes de uma vontade consciente, analisando o produto das possibilidades pelas intenções (Couto, 1988), podendo provocar desta forma alterações em termos da segurança do ou dos sistemas.

Embora o conceito de **segurança** seja alvo de uma ampla discussão, o termo em si tem origem no latim se+cura, significando "sem preocupações". Em termos mais abrangentes, podemos considerar segurança como a busca da libertação relativamente à ameaça, sendo a resultante da interação entre as vulnerabilidades de uma unidade política e as ameaças que a mesma enfrenta (Weaver, 1993).

Definidas estas noções, interessa agora aprofundar a questão do Risco.

3.1. Risco

Conforme refere Gonçalves (2010), a noção de risco tem origem no latim medieval resicum, noção que seria aplicada em contextos associados a atividades marítimas e à lei comercial marítima (Piron, 2004), sintetizando a presença simultânea de incerteza, oportunidades e ameaças numa situação sistémica.

Segundo Gonçalves (2010**,** p.11)**: "**(…) a noção de risco é um nome para uma situação sistémica concreta ligada ao mecanismo de vida e morte, e na qual os mecanismos homeostáticos de um sistema desempenham um papel projetivo fundamental no que diz respeito à possibilidade de antecipação e adaptação a ocorrências futuras, enraizadas e condicionadas pela configuração da situação sistémica na qual tiveram origem, e que transportam consigo ameaças à integridade sistémica e/ou oportunidades de expansão das condições de sobrevivência do sistema. Uma tal situação sistémica é designada, por situação de risco. Uma situação de risco, tal como esta noção é trabalhada na ciência do risco, é, assim, uma situação sistémica em que existe incerteza, oportunidades e ameaças."

Sendo a probabilidade uma medida humana, uma ferramenta de cálculo, não faz parte de uma ontologia sistémica ao contrário do risco. O risco, em termos fundamentais é, necessariamente, dissociável da probabilidade.

A noção de risco é objeto de estudo científico em dois campos: a ciência (geral) do risco (que conta com já vários institutos de investigação que lhe são dedicados[81]); a matemática do risco (que serve de suporte formal à ciência do risco).

Na gestão e economia, o estudo do comportamento dos mercados, trabalharam em dado momento, a partir de noções de risco vindas do seio da teoria matemática da decisão e da teoria dos jogos, tendo agora, deslocado para a ciência do risco e para a matemática do risco a fonte de base de tratamento científico.

Relativamente à medição de risco, não existe uma medida geral para o risco, existem medidas de risco, diferentes, conforme os contextos**,** e que são desenvolvidas numa vasta literatura da matemática da medição do risco, subramo da matemática do risco (Gonçalves, 2010).

Com o desenvolvimento da ciência do risco, e com base no trabalho do **World Economic Forum** acerca do **Risks Interconnection Map**, reorientou-se o discurso científico acerca do risco nos sistemas para uma classificação operativa em termos de domínios. Assim não se trata tanto de uma afetação exclusiva de um "espaço material" mas de uma afetação global que envolve os diferentes domínios de risco: sociais, económicos, geopolíticos, ambientais e tecnológicos[82].

Os resultados desta abordagem de avaliação de risco seguida pelo **World Economic Forum**, baseada na ciência do risco, visa orientar o planeamento estratégico apoiando a definição das linhas de ação a seguir, as medidas a serem implementadas e as prioridades a serem estabelecidas para a gestão de risco em situações de risco interconectado.

Estabelece-se um processo de avaliação de riscos que deve incluir uma abordagem sistemática, que permita estimar a magnitude dos riscos (análise de risco) e o processo de comparar os riscos estimados com base em critérios de nível de ameaça e de contaminação dinâmica.

No que se refere à questão do risco associado à **Nova Pangeia**, interessa refletir em termos globais sobre este sistema, tentando perceber o seu impacto, na sociedade e nos indivíduos**,**

81 Tais como: University of Michigan com o seu Risk Science Center dedicado a questões relacionadas com a saúde, (mais informação em: http://www.sph.umich.edu/riskcenter/) ou Southampton Management School com o seu um Centro de Investigação de Risco criado em 1990 com o objectivo de promover e incentivar o estudo do risco de forma interdisciplinar (mais informação em: http://www.southampton.ac.uk/management/research/groups/centre_for_risk_research.page).
82 Fontes: Disponíveis para consulta em: http://newschoolsecurity.com/wp-content/uploads/2010/03/rimap.jpg - e - http://newschoolsecurity.com/2010/03/risks-interconnection-map/

avaliando as suas possíveis forças, fraquezas, ameaças e oportunidades, apresenta-se a seguinte análise:

Tabela 1 - Análise "SWOT" – Nova Pangeia

Forças	**Fraquezas**
• Movimento Global • Massificação de formas e dispositivos que a utilizam • Eliminação de Fronteiras • Rápida capacidade de proliferação da informação e do conhecimento	• Necessidade de especialização para o seu uso • Maior complexidade das relações Homem – máquina e vice-versa • Perigo de isolamento tecnológico
Oportunidades	**Ameaças**
• Mercados Globais • Redução teórica geral dos preços • Maior acesso à informação e ao conhecimento • Menos importância do fator localização • Nova noção de comunidade	• Maior importância da especialização e do conhecimento • Maior facilidade de entrada de novos competidores • Maior risco de Infoexclusão • Demasiada dependência das sociedades modernas da Nova Pangeia

A Internet e o subsequente desenvolvimento da Nova Pangeia impulsionou um movimento global, facilitando e estimulando a ligação entre povos. Nesta interconexão quase planetária, reside uma das suas maiores forças, este movimento global que se massifica abrangendo cada vez mais dispositivos e indivíduos à medida que avança elimina fronteiras, facilitando a circulação de informação e conhecimento num movimento que torna agora possível a comunicação e a realização de transações a uma escala nunca antes experimentada.

Contudo existem fraquezas, fundamentalmente barreiras que impedem a conexão ou dificultam a ligação ao sistema Nova Pangeia. Assim a sua não disponibilidade ou universalidade, a complexidade de uso ou necessidade de formação para a sua utilização, são barreiras que dificultam a entrada ou acesso ao sistema, aumentando o risco da não inclusão ou exclusão tecnológica, o que pode gerar o isolamento forçado. Numa sociedade cada vez

mais conectada e em rede, traduz-se em maiores dificuldades de acesso a informação e conhecimento.

Naturalmente que as oportunidades geradas pela formação de mercados globais, que facilitam as trocas, aumentando a competitividade e a cooperação, geram uma maior proximidade entre a oferta e a procura, o que se pode traduzir numa redução tendencial de preços, ou pelo menos num maior leque de escolhas. Por outro lado o maior acesso à informação e ao conhecimento pode manifestar-se numa sociedade mais esclarecida e avisada, sendo mais fácil chegar também ao seu contacto.

O sistema Nova Pangeia facilita a criação de uma nova noção de comunidade, a comunidade on-line, que normalmente se reúne em torno de tópicos de interesse comum e se cruza pelas ligações e trocas de informação que realiza.

A cada vez maior importância da especialização e do conhecimento traduz-se num esforço adicional que pode levar a uma utilização errada do sistema. Por exemplo, um utilizador não avisado, ou que não domine a tecnologia, pode aceitar divulgar os seus dados, pondo em risco a sua conta bancária.

Este sistema, Nova Pangeia, facilita a entrada de novos competidores, embora isso leve a um aumento da cooperação, pode tornar-se uma ameaça.

À medida que o sistema Nova Pangeia se expande, torna as sociedades mais dependentes da tecnologia, em alguns sectores de atividade, quase totalmente, como por exemplo os mercados financeiros. Quando o sistema colapsa as transações param e o sistema não funciona. Esta maior dependência das sociedades atuais, da Nova Pangeia, pode ser considerada como uma das principais ameaças.

Se por outro lado, tivermos em conta os casos dos ataques à Estónia**,** em Abril e Maio de 2007[83], podemos compreender que a *Nova Pangeia* conduz a diversos riscos/ameaças, que estão além da inquestionável importância que esta representa para a sociedade atual.

Importa assim realizar um levamento que permita identificar um conjunto de riscos que podem ter origem a partir ou neste sistema Nova Pangeia.

3.2. Análise de Ameaças às infraestruturas da Nova Pangeia

Inspirado pelo World Economic Forum no seu "Global Risks Report 2012" e tendo como base fundamental o trabalho desenvolvido por Gonçalves e Madeira (2009) recorre-se ao uso de uma teia *mórfica* para a cenarização, avaliação de fontes de risco e ameaças às infraestruturas da Nova Pangeia.

83 Nota: Ver Capítulo 4

Assim com base na teoria matemática das *teias mórficas*, que expande a teoria matemática das categorias, introduzida por Gonçalves e Madeira (2009)[84], no contexto da cibernética matemática, e expandida por Gonçalves (2010), como base para uma linguagem matemática subjacente a uma matemática do risco fundamentada na base paradigmática da quarta fase de desenvolvimento da cibernética, recorre-se ao uso de metodologias e ferramentas que resultam destas noções matemáticas.

Ainda com base no trabalho de Gonçalves (2012a) e *teia mórfica* proposta no modelo: *Cyber Threats to Global Governance Risk Web*[85], far-se-á a construção de uma *teia mórfica,* que permita identificar ameaças e avaliar**,** mediante a construção de cenários**,** o impacto e risco que estas fontes representam para o sistema, tentando inferir do seu potencial de colapso.

Interessa pois em primeiro lugar, e tal como Gonçalves (2012b) fez, definir colapso. Assim citando: "Colapso, do latim *collapsus*, *cum+labi* (cair em conjunto), é uma questão formativa central da ciência do risco, que se intersecta com a problemática conceptual das ciências da complexidade e da ciência dos sistemas (…) Um ponto central da cibernética e das ciências da complexidade, presente também ao nível da ciência do risco, é o de que não há nenhum sistema imune ao colapso (…) O colapso sintetiza, ao nível dos sistemas, dinâmicas de rutura (do latim *ruptura/rumpere*: quebra de estrutura) (…)"

A questão do colapso é incorporada no contexto da ciência do risco, metodologicamente, em termos de uma abordagem necessária à construção de cenários e ao desenvolvimento de estratégias potenciadoras de fatores de sustentabilidade.

As *teias mórficas***,** conforme Gonçalves (2010)**,** são no contexto matemático**,** redes compostas por objetos e morfismos, em que um morfismo é definido a partir de uma noção elementar e sistemicamente constitutiva de movimento de uma *origem* para um *alvo*, tal que uma conexão mórfica é uma conexão dirigida da origem para o alvo (Gonçalves e Madeira, 2009; Gonçalves, 2010).

Para analisar as ameaças às infraestruturas da Nova Pangeia, procede-se à construção de uma *teia mórfica*, colocando-se num ponto central as infraestruturas da Nova Pangeia, inventaria-se um conjunto de ameaças significativas que seguidamente se apresenta, formando uma

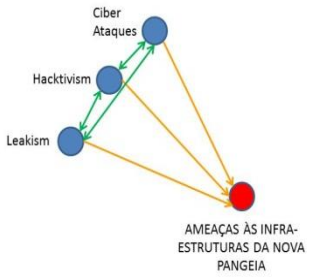
84 Nota: Sugere-se consulta - A Systems Theoretical Formal Logic for Category Theory", 2009, Gonçalves, C.P. and Madeira, M.O., informação disponível para consulta em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396841)

85 Nota: Modelo proposto por Gonçalves a partir do artigo Risk Governance - A Framework for Risk Science-Based Decision Support Systems (Gonçalves, 2012a), e incluído contexto do projecto Risk Governance na plataforma Modelling Commons do The Center for Connected Learning and Computer-Based Modeling da Northwestern University:
http://modelingcommons.org/browse/one_model/3423#model_tabs_browse_info,
http://riskgovernancestrategy.blogspot.pt/2012/07/cyber-threats-to-global-governance-risk.html.

rede global de ameaças, que se particularizará na construção de sete cenários principais de risco.

O nó central será apresentado a vermelho, sendo que os restantes nós se encontram agrupados em cores diferentes por forma a configurarem conjuntos de similares, a ligação é feita através de setas de ligação, que serão verdes sempre que a relação mórfica for bidirecional e cor de laranja quando apenas for unidirecional.

Figura 6 - Cenário 1



No caso de um Ciber Ataque com dimensão, as infraestruturas da nova Pangeia podem colapsar, ficar bloqueadas ou com serviços afetados ou diminuídos, impedindo comunicações, ou até provocar implicações noutros sistemas podendo desencadear situações de risco fora do sistema Nova Pangeia o que explica a ligação do nó "Ciber Ataques" para o nó "Ameaças às Infraestruturas da Nova Pangeia".

Se tivermos em atenção os acontecimentos de Abril e Maio de 2007 na Estónia, a apresentar no Capitulo 4, rapidamente podemos constatar a forma como as infraestruturas da nova Pangeia entraram em colapso, num cenário semelhante ao apresentado.

Primeiro, com dificuldade de acesso à Internet e às comunicações em geral, motivada pelos inúmeros ataques de *DDOS-Distributed Denial of Service* e *SPAM*, numa primeira fase causando um acesso lento aos servidores e aos serviços baseados na Internet.

Com o escalar da situação, o acesso aos serviços de Internet passou da lassidão para um estado de bloqueio com certos serviços inacessíveis, quer do Estado quer privados, criando uma situação de colapso e não resposta do sistema.

Fruto destes ataques, outros serviços fora da Nova Pangeia foram afetados, caso das comunicações fixas e móveis, que em certas partes do país ficaram inacessíveis, bloqueadas pelos efeitos do ataque desencadeado, conforme podemos verificar no estudo de caso, apresentado no Capítulo 4.

Para além do referido exemplo da Estónia, outros exemplos têm-se registado em que os Ciber Ataques produzem efeitos fora do sistema Nova Pageia.

Recentemente**,** o *Stuxnet*[86]*,* primeiro *worm*[87] conhecido como tendo sido desenvolvido para atacar redes *SCADA*, pode ilustrar mais profusamente uma situação de risco intersistémico.

Este *worm,* quando infiltrado na rede *host* através da mutação dos seus códigos, permitiria que os atacantes tomassem controlo do sistema/sistemas sem que os operadores ou utilizadores se apercebessem.

Segundo a *Homeland Security News Wire (2013)*, este worm foi empregue no âmbito de uma operação conjunta EUA-Israel com o nome de código Olympic Games, aprovada diretamente pela presidência dos EUA e implementada pela NSA (National Security Agency).

O *worm* foi inicialmente utilizado com o objetivo de atacar a indústria nuclear iraniana de enriquecimento de urânio, infiltrando-se na rede, gravando dados telemétricos da operação da central nuclear, propagando-se de forma a poder influenciar e gerar comandos na rede SCADA da central, fazendo com que as unidades centrífugas girassem 40% mais rápido durante quinze minutos, causando brechas nessas unidades que as levariam ao seu colapso. Naturalmente que todas estas operações seriam encobertas dos operadores/utilizadores, pela apresentação de dados/informações falsas nas consolas de gestão do sistema, escondendo e camuflando a falha.

Este ataque ilustra de sobremaneira o potencial que um Ciber Ataque pode representar, quer para a Nova Pangeia, quer para os sistemas fora dela, sendo uma fonte principal de risco e criando uma ligação de causalidade intersistémica, o que amplifica o seu potencial estratégico.

Neste cenário é apresentado também o hacktivism[88], como uma fonte de risco, na medida que poderá ser uma força de bloqueio ao sistema, uma manobra de subversão ou uma fonte inspiradora de ações de protesto contra o sistema, ou ordem estabelecida, podendo levar à sua inoperabilidade e também ao seu colapso.

Recorrendo mais uma vez ao caso de estudo da Estónia, podemos encontrar**,** nos antecedentes deste ataque, manobras primeiro de ativistas que na rua manifestam o seu descontentamento e oposição contra a situação, que rapidamente são seguidos por "hacktivists", no ciberespaço**,** por intermédio de *posts* em blogues, intervenções em fóruns, conferência em salas de *chat,* instigam ao radicalismo e a que sejam tomadas ações de

86 Nota: Ver mais informações disponíveis em http://www.symantec.com/pt/br/theme.jsp?themeid=stuxnet
87 Nota: *worm* - programa que se auto replica de forma rápida e de fácil propagação depois de infiltrado num sistema.
88 Definição – "Hacktivistas", que corresponde à junção do "Hacker" com ativista, termo atribuído a Jason Sack (1995), significando o uso ou recurso a estratégias e tácitas on-line, próximas da tradição anarquista autónoma, aplicando o uso de "hacking" à política e ao ativismo não-violento. Como qualquer outra forma de ativismo, as perceções são sempre diferentes; alguns vêm o hacktivismo como uma ferramenta necessária contra a opressão ou sistema, outros como uma forma ilegal de manifestação.

natureza violenta e subversiva. Criam num primeiro instante uma força de bloqueio, apoiam e formam uma corrente de opinião contra o Estado e suas intenções.

Estes protestos no ciberespaço rapidamente criam as condições ideais para que os Ciber Ataques sejam lançados, dando cobertura e funcionando como agentes facilitadores da manobra, criando assim uma relação entre estas duas fontes de risco que**,** em conjugação, levaram à inoperação e colapso de partes do sistema.

Recentemente com os acontecimentos no Egipto, na chamada Primavera Árabe, o hacktivism assumiu um papel determinante na mobilização das massas, na formação de opinião e corrente subversivas, no favorecimento de ações contra o Estado, quer dentro quer fora do sistema Nova Pangeia.

A extensão da ameaça e o risco foi tal que o Governo Egípcio bloqueou o acesso à Internet durante 5 dias, como forma de silenciar os protestos no Ciber Espaço e impedir a sua proliferação, contendo a informação e tentando impedir quer a mobilização de protestos ou ações contra o Estado.

Segundo a Organização para a Cooperação e Desenvolvimento Económico (OCDE), o corte da Internet deverá ter custado ao país 65 milhões de euros.

Temos aqui mais uma ligação de causalidade intersistémica.

Por seu turno, o leakism, terceira fonte de risco identificada no cenário 1**,** é causa de ameaça para o sistema, uma vez que a divulgação de informações, classificadas ou de âmbito da segurança nacional**,** bens ou recurso estratégico, podem perturbar a ordem e o funcionamento do sistema.

Embora seja um fenómeno recentemente mediatizado, a fuga de informação teve sempre uma importância estratégia, quanto mais valor tiver a informação revelada, maior potencial de ameaça representará.

A revelação de mais de 200.000 telegramas diplomáticos trocados entre o Departamento de Estado dos EUA e as suas missões diplomáticas poderia ter sérias implicações para a diplomacia dos EUA e para a guerra liderada pelos EUA contra o terror, afetando as suas operações e altos funcionários de Estado (Global Geopolitics & Political Economy, 2010)

Com efeito, o embaraço diplomático, causado pelo episódio *Wikileaks*, é revelador da importância desta fonte de risco.

Em primeiro lugar**,** pela facilidade de acesso à informação, em poucos segundos, biliões de utilizadores em todo o mundo podem ter acesso à informação, revelando-se assim outro fator que é a velocidade potencial que a dinâmica pode atingir, em instantes, documentos

classificados e importantes podem cair nas mais variadas mãos irreversivelmente, revelando informação sensível a diversos níveis.

A real dimensão deste caso é por enquanto difícil de apurar, naturalmente que diplomaticamente o Estado e os serviços de informação dos EUA foram afetados, quer na sua credibilidade, quer pela fragilidade exposta nos seus protocolos de segurança, o que invariavelmente comprova o risco que esta ameaça tem para o sistema em si e para outros sistemas.

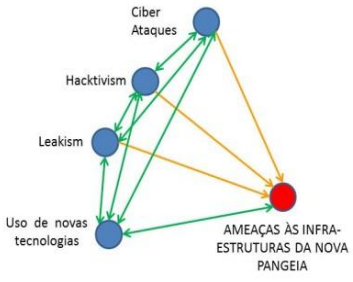
Todas as fontes de risco apresentadas neste primeiro cenário podem estabelecer relações entre si de uma forma multidimensional e intersistémica, conforme Ilustração do Cenário 1.

Os Ciber Ataques podem provocar o leakism mas também podem ter origem nele. Hipoteticamente pode-se até considerar que todas as fontes de risco apresentadas neste cenário podem, também, ocorrer simultaneamente inter-influenciando-se e amplificando as suas ações/efeitos provocando um efeito de contaminação na rede, que pela sua conjugação poderá ter um efeito muito maior.

Por hipótese: um determinado ataque pode começar pela revelação de uma informação, essa fuga/leak, por sua vez gera um movimento de contestação, hacktivism, que impele à revolta apelando a Ciber Ataques contra determinados alvos, como forma de retaliação ou como forma de provocar dano, e recorrendo a diversos meios, exemplo os utilizados no caso da Estónia, DDOS causam uma inoperação do sistema podendo provocar o seu colapso.

Esta combinação, embora hipotética e simplificada, é reveladora da capacidade com que estas fontes de risco podem afetar o sistema, revelando assim o seu potencial de risco estratégico.

Figura 7 - Cenário 2



No Cenário 2, é adicionado um novo nó correspondente ao uso de novas tecnologias, sendo que a relação estabelecida com as infraestruturas da Nova Pangeia é uma relação mórfica bidirecional, por um lado**,** o uso de novas tecnologias pode provocar efeitos desconhecidos nas infraestruturas do sistema, podendo desencadear a sua degradação ou até mesmo o seu colapso. Por outro lado**,** o seu uso nas infraestruturas da Nova Pangeia pode levar a evoluções ou até ao seu crescimento. Veja-se a introdução de redes de fibra ótica, em que o salto obtido aquando da introdução desta nova tecnologia foi de extrema importância, permitindo que as infraestruturas da Nova Pangeia, fossem mais rápidas e tivessem mais capacidade de transporte.

As novas tecnologias encontram, nesta infraestrutura o meio ideal para se poderem propagar, veja-se o efeito de um vírus ou *malware*, enquanto a sua ação é desconhecida vai causando danos no sistema. Esse vírus ou *malware* pode causar danos mas também pode produzir degradações de serviço nas infraestruturas da Nova Pangeia.

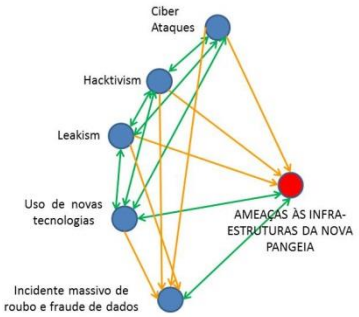
Conforme reconhece Paganini (2012)**,** a exploração de uma nova vulnerabilidade é uma prerrogativa do trabalho de um *Hacker*, essa busca constante leva ao desenvolvimento de novas técnicas e capacidades que muitas vezes se transformam na descoberta e uso de novas tecnologias.

Como exemplo recente da eficiência de uma arma cibernética podemos analisar os dados relacionados com a propagação do Stuxnet. Uma fonte interessante sobre o tema é: "Symantec W32.Stuxnet Dossier Versão 1.4 (Fevereiro de 2011)", que fornece estatísticas e informações úteis sobre a infeção desencadeada nessa altura por uma nova tecnologia, o Stuxnet [89]. Este ataque teria a capacidade de produzir danos em infraestruturas críticas, neste caso relacionadas com a energia podendo inclusivamente causar, como referido no cenário anterior (1), a explosão de um reator nuclear, ou provocar disrupções energéticas capazes de afetar serviços do Estado. Este cenário mais extremo foi, segundo a Homeland Security[90], travado pelo Presidente Obama determinando de que os ataques fossem suavizados (*watered down*) de tal modo que as disrupções energéticas não produzissem os efeitos acima referidos, contudo, conforme a informação da Homeland Security a arma pode ser utilizada para produzir esse tipo de efeitos extremos.

A mesma situação é válida para todas as componentes deste cenário. Ou seja, o uso de novas tecnologias pode desencadear um conjunto de Ciber Ataques, ataques esses que podem ser realizados porque essa tecnologia se encontra disponível. Por exemplo, essa nova tecnologia pode ter sido conhecida com base na fuga de uma informação, caso de leakism, ou fruto de uma manobra de hacktivism, que nesta nova tecnologia encontra uma forma mais eficaz de manifestar as suas ações ou intenções.

89 Nota: considerado como a primeira arma cibernética por muitos especialistas e já referido anteriormente.
90 Fonte: Informação disponível para consulta on-line em: http://www.homelandsecuritynewswire.com/dr20130206-u-s-cyberstrikes-against-adversaries-to-require-presidential-authority

Figura 8 - Cenário 3



No cenário 3**,** é adicionado um novo nó correspondente a situações de *incidentes massivos de roubos e fraude de dados.* Temos uma situação ligeiramente diferente das anteriores, uma vez que os incidentes massivos de roubos e fraude de dados têm uma relação bidirecional com as Ameaças às Infraestruturas da Nova Pangeia, uma vez que esses dados, ou a sua fraude, podem ser utilizados para infligir danos, provocar roubos ou causar o colapso de um determinado sistema, como por exemplo o financeiro.

De igual modo**,** um evento de disrupção ao nível das infraestruturas da Nova Pangeia pode deixar vulnerabilidades que podem ser exploradas, permitindo o acesso a informação e a dados que indevidamente são acedidos, expostos ou usados em larga escala, dando assim origem a incidentes massivos.

Em Março de 2012**,** VISA e MasterCard alertaram os bancos nos EUA sobre uma violação e fuga massiva de dados num dos maiores processadores de cartões de crédito dos EUA (White, 2012), que teria comprometido cerca de 10 milhões de números de cartões.

Este ataque realizado por *Hackers* a esses processadores de cartões de crédito poderia significar que informação seria usada para produzir novos cartões falsificados, levando ao seu uso em operações financeiras indevidas, que caso não fossem identificadas**,** poderiam**,** em larga escala**,** causar danos assinaláveis ao sistema financeiro, produzindo efeitos noutros sistemas.

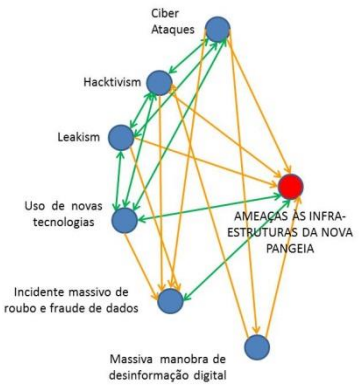
Já em 2013, numa investigação dirigida pela Global Research & Analysis Team (GReAT) da empresa Kaspersky Lab, descobriu aquela que poderá ser uma das maiores operações de Ciber-Espionagem até agora encontrada, conhecida como *"The Red October Campaign" (GReAT, 2013).* Durante cinco anos (2007-2012), esta operação/esquema de roubo massivo de informação e dados, infiltrou-se em redes de computadores de organizações de investigação, diplomáticas, governamentais e científicas, reunindo dados e informações a partir de dispositivos móveis, sistemas de computadores e equipamentos de rede.

A equipa de especialistas da Kaspersky Lab concluiu que o esquema usado, disfarçado num *malware* em forma de documento, estava infetado com ferramentas que exploravam pontos fracos do sistema permitindo a intrusão e o acesso a dados e informações privilegiadas.

Como principais alvos**,** destacam-se organizações específicas situadas principalmente na Europa Oriental, Estados ex-membros da URSS e países da Ásia Central, mas também na Europa Ocidental e América do Norte.

Temos assim dois exemplos em que a relação estabelecida com os restantes nós é unidirecional, uma vez que normalmente é uma consequência das outras situações de risco presentes no sistema, que podem desencadear esta situação.

Figura 9 - Cenário 4



O Cenário 4 desenvolve-se com a adição da massiva manobra de desinformação digital, semelhante à manobra tradicional de *psy-ops*, sendo uma fonte de risco para o nó central, uma vez que pode prejudicar o seu funcionamento com base em falsas informações que podem levar a um movimento de protesto e sucessivamente criar colapso no sistema.

Um dos exemplos de manobra de desinformação digital mais comum é tecnicamente denominada por *deface* ou *defacement*[91].

O *defacement* é uma ação utilizável para manobras de desinformação, mas importa notar que a desinformação corresponde a uma manobra tácita de divulgação de informação falsa com fins estratégicos, nesse sentido, a conexão com a *psyops* ou a *psyops digital* é significativa.

Esta técnica é comummente utilizada recorrendo ao uso de *SQL injection exploits*[92]*,* sendo que tem atingindo os mais diversos *sites* de internet.

Como exemplo relevante podemos apresentar o defacement da página oficial de Mikheil Saakashvili´s:

91 Nota: Técnica que consiste na alteração de conteúdos oficiais publicados pelos donos da informação, proprietários ou afiliados autorizados de um determinado site ou domínio**,** substituídos por conteúdos, imagens, textos, ferramentas ou formas de páginas ou portais Internet não oficiais, ou não autorizadas pelos respetivos donos da informação, proprietários ou afiliados autorizados de um determinado site ou domínio.
92 Nota: Técnica que permitem aos atacantes adicionar o seu próprio código ao site alvo pela exploração de falhas relacionadas com Base de Dados.

Figura 10 - Defacement da página oficial de Mikheil Saakashvili's

(Fonte Imagem – Retirada ZDNET.COM – Em: http://cdn-static.zdnet.com/i/story/60/80/001670/georgia_ddos3.JPG)

O *site* oficial de Mikheil Saakashvili, presidente da Geórgia em 2008, foi vítima de *defacement* tendo sido substituído por uma apresentação de slides retratando Mikheil Saakashvili como Hitler, opondo imagens suas em contraponto às de Hitler.

Este ataque foi atribuído pelo Ministro dos Negócios Estrangeiros da Geórgia à Rússia**,** tendo este por essa ocasião proferido as seguintes declarações: "Uma campanha de *cyber warfare* realizada pela Rússia está a afetar seriamente muitos *sites* da Geórgia, incluindo o do Ministério dos Negócios Estrangeiros." (Danchev, 2008)

Estes ataques precederam a intervenção da Rússia na Geórgia, em 2008, sendo que são considerados como fazendo parte da vasta manobra ofensiva lançada pela Rússia a este País e estendendo o teatro de operações ao Ciber Espaço, sendo este caso, simultaneamente**,** um exemplo de manobra de desinformação e um Ciber Ataque.

Esta técnica estabelece uma relação de fonte de risco quer com os Ciber Ataques, que normalmente recorrem ao uso desta manobra como ataque em si, quer com o *hacktivism*, como podemos constatar nos exemplos anteriores.

Por outo lado**,** o l*eakism* também pode ser uma via de desinformação, se o *leak* for falso.

Uma das formas mais usadas para manipulação e manobras de informação/desinformação são os fóruns, as comunidades de discussão, *sites* com abertura para comentários e as redes sociais, onde “operacionais”, contratados ou mandatados por terceiros, podem manipular a rede a favor dos seus interesses ou dos interesses que representam, manipulando a opinião pública com permanentes manobras de informação/desinformação.

(Fonte Imagem – por Luke Hopewell/ZDNet Austrália em Agosto de 2011)

Figura 11 - Anonymous Defacement da página do Ministro da Defesa Sírio

Como exemplo podemos destacar o caso apresentado na Figura 11 - Anonymous Defacement da página do Ministro da Defesa Sírio. No fundo da bandeira síria, mostrou-se**,** em vez do *site* do ministério, uma mensagem anti governo e um bloco de vídeos do YouTube que alegadamente ilustra casos de brutalidade militar, perpetrados por este regime.

Neste exemplo, podemos encontrar para além do *defacement,* dado que a página oficial foi alterada, uma manobra de *cyber psyops* que se serve de *hacktivism* para denúncia de factos, não sendo uma situação totalmente de desinformação, pois a informação divulgada é verídica.

O potencial de risco destes ataques fica demonstrado, não só por violar uma página oficial de um organismo de Estado, supostamente mais seguro, mas também pela capacidade de difundir mensagens através desse meio podendo estas serem consideradas verdadeiras e por isso, gerarem outro tipo de ações ou movimentos.

Figura 12 - Defacement ao Jornal The Sun declara morte de Rupert Murdoch

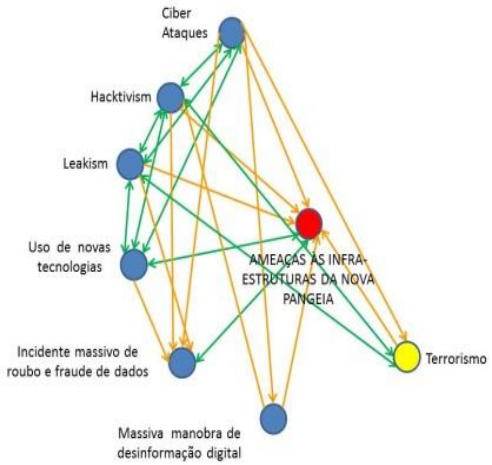
(Fonte Imagem – Retirada do Site da Forbes em: http://blogs-images.forbes.com/andygreenberg/files/2011/07/murdochdead.png)

Um dia depois da prisão de Rebekah Brooks, presidente-executivo da New Corp, e editor do jornal The Sun, um grupo de Hackers (Anonymous e LulzSec) reclamou o *defacement* do site do jornal redirecionando tráfego para uma página falsa, que anunciava que o proprietário da News Corp**,** Rupert Murdoch, havia morrido de uma overdose de drogas (Greenberg, 2011).

Este exemplo ilustra a capacidade de afetar o sistema que estes esquemas/operações têm. Trata-se de um dos jornais mais lidos em Inglaterra e um dos mais visitados pelo exterior. Embora se tenha tratado de uma ação de retaliação, e a notícia seja algo inócua em termos de ações subsequentes, fica demostrado o potencial de desinformação, uma vez que a sucessiva passagem de notícias falsas ou manipuladas pode gerar ações em partes ou em todo o sistema em si.

O efeito destas ações para o sistema pode funcionar como uma bola de neve, podendo atingir uma dimensão tal, que afete o sistema no seu todo ou em parte.

Figura 13 - Cenário 5



No Cenário 5, introduz-se um conjunto de ameaças, que não são "puramente digitais" como as descritas anteriormente, com a introdução de um novo nó para o Terrorismo.

Num primeiro momento, o Terrorismo é uma fonte de risco para o nó central uma vez que o seu efeito pode ser devastador, imagine-se um ataque terrorista, dito convencional, em larga escala, que destruísse diversos *POPs*, operadores de comunicações, a própria infraestrutura da Nova Pangeia estaria em perigo nesses determinados locais e o seu acesso degradado ou vedado.

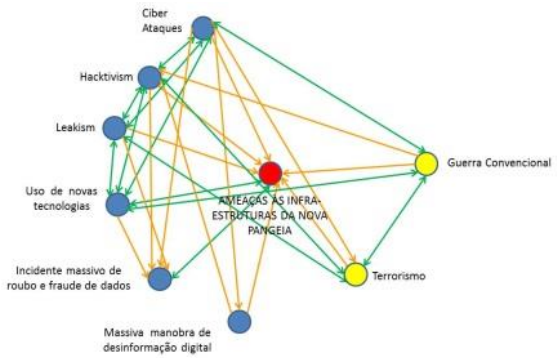
Por seu turno, um massivo Ciber Ataque do tipo DDOS, como os realizados contra a Estónia gerando o colapso de partes da rede de comunicações, realizado por um grupo de Ciber Terroristas, teria também um efeito devastador no nó central.

Podemos assim, inferir que os Ciber Ataques podem ser formas de manifestação de ambas as ameaças, pois neles podemos encontrar uma forma de estas se efetivarem.

Como paradigma deste cenário refira-se o apelo da Al Qaeda para a chamada '*Electronic Jihad*' (*Cloherty, 2012).*, neste caso, temos uma chamada de ação para a guerra eletrónica contra os EUA, que surge como uma forma de criação de um movimento de *Hacktivism* muçulmano contra interesses dos EUA, que deverá utilizar todos os meios eletrónicos ao seu alcance para prejudicar os EUA.

Por outro lado, o *leakism* poderá ser gerador de Terrorismo, na medida em que informações libertadas sobre uma determinada matéria podem gerar um movimento de contestação que conduza a ações Terroristas, ou ao Terrorismo em si mesmo, pode desencadear um movimento de *leakism* forçando a libertação de informação que, pelo efeito de uma ação terrorista, a liberta ou torna conhecida.

Figura 14 - Cenário 6



No sexto cenário introduz-se um novo nó, a Guerra Convencional justificando-se plenamente pelas múltiplas conexões que podem ser estabelecidas com as restantes situações de risco.

Em primeiro lugar, existe uma relação de fonte de risco desde logo com o nó central. Tal como o terrorismo, o seu efeito pode ser devastador para as infraestruturas da Nova Pangeia, uma vez que o seu poder de destruição pode causar múltiplos impactos. Imagine-se um ataque a centrais de produção de energia ou até mesmo a operadores de telecomunicações**,** a Nova Pangeia**,** que pela destruição dessas infraestruturas**,** poderia colapsar.

Por outro lado**,** a Guerra Convencional poderá ser fonte de *hacktivism*. Ser fonte de risco para o *hacktivism* significa que ameaça o *hacktivism*, ou seja, tem por alvo capturar ou neutralizar os grupos *hacktivistas*, ser fonte de *hacktivism* significa que pode conduzir a *hacktivism* sem ligação com um Estado ou uma qualquer fação envolvida num conflito, assim como pode ocorrer *hacktivism* enquanto forma de ocultação da ação militar de um Estado contra outro (ou de uma fação envolvida num conflito militar convencional contra outra fação), isto é, um Estado atacante pode servir-se do *hacktivism* como manobra de disrupção escondendo simultaneamente a sua atuação por detrás das ações de um grupo *hacktivista*, de tal modo que as *cyber ops* não são identificadas diretamente com o Estado atacante, dificultando uma previsão por parte da *intelligence* e dos centros estratégicos do Estado alvo de um ataque convencional após os Ciber Ataques.

Durante o conflito do Kosovo (Arquilla & Ronfeldt, 2001), Organizações e indivíduos em todo o mundo usaram *sites* de Internet**,** *blogs* e fóruns para publicar informações relacionadas com o conflito sendo que, em alguns casos, solicitavam apoio e instigavam a tomarem posições e a protestarem, numa posição clara de *hacktivism*.

Podemos ainda estabelecer relações entre a guerra convencional bidirecionais com as seguintes situações sistémicas: terrorismo**,** uso de novas tecnologias e Ciber Ataques.

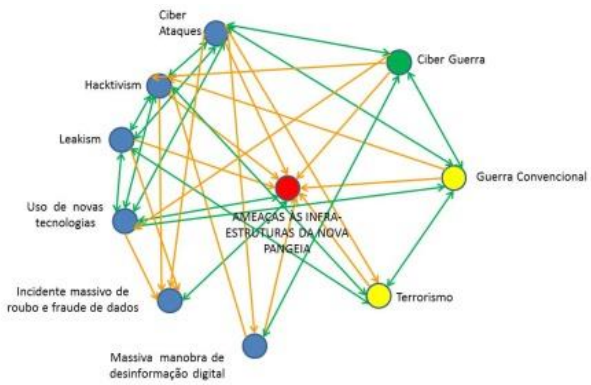
No caso do terrorismo, um exemplo paradigmático é o dos acontecimentos de 11 de Setembro, com os ataques às Torres Gémeas, iniciando-se a Guerra ao Terror ou Guerra ao Terrorismo[93].

93 Nota: iniciativa militar desencadeada pelos EUA, fruto da doutrina do seu então Presidente, George Bush, que conduziu à invasão e ocupação do Afeganistão e do Iraque.

Em sentido contrário, a guerra convencional pode desencadear ataques terroristas, veja-se o exemplo dos múltiplos atentados perpetrados no Afeganistão contra as tropas da NATO.

Por outro lado**,** uma manobra de guerra convencional pode utilizar um Ciber Ataque como uma arma. No caso da Geórgia**,** por exemplo, em 2008, antes da intervenção terrestre da Rússia diretamente no país, muitas semanas antes**,** no Ciberespaço, a Rússia desencadeava já ações de preparação da manobra terrestre (Danchev, 2008), usando esta nova tecnologia como uma ferramenta de desestabilização, numa primeira fase, e depois de ataque a interesses do Governo Georgiano, utilizando diversas técnicas de DDOS para colapsar alguns sectores do país.

Figura 15 - Cenário 7



No cenário 7 introduz-se a Ciber Guerra, dada a relevância e múltiplas conexões que podem ser estabelecidas com as restantes situações de risco presentes no sistema, destaca-se este nó com utilização de uma nova cor (verde).

Podemos tomar como ponto de partida para a explicação de Ciber Guerra, em termos de objetivo, próxima da Guerra dita convencional, ou seja a Ciber Guerra, tendo como objetivo a derrota, submissão, ou paralisação estratégica do adversário, utilizando para isso a Nova Pangeia.

A Ciber Guerra, como já referido anteriormente, tem cada vez mais uma relação direta com a Guerra Convencional e pode expressar-se através de Ciber Ataques, que por sua vez podem recorrer a manobras de desinformação digital, a Roubo e Fraude de Dados, e procurar nos movimentos de hacktivism uma extensão ou forma para atingirem um determinado objetivo. Temos assim um nó que se pode apoiar ou até utilizar todas as fontes de risco presentes no sistema para colapsar ou afetar o sistema Nova Pangeia em si.

Veja-se o referido caso da Geórgia em 2008, em que todas estas situações de risco se encontram presentes.

Com base nestas ligações, podemos compreender a ameaça que representa para o sistema Nova Pangeia, uma vez que as suas ligações são mais extensas e podem abranger os diversos nós, a sua perigosidade para o sistema é naturalmente maior tendo mais impacto em termos de risco.

4. CAPÍTULO – ESTUDO DE CASO - ESTÓNIA ACONTECIMENTOS DE ABRIL E MAIO DE 2007

Neste Capítulo apresenta-se o Estudo de Caso da Estónia, e os acontecimentos de abril e maio de 2007, analisando-se os acontecimentos em Tallinn, no ciberespaço e as implicações lógicas e físicos que estes ataques procuraram.

4.1. Breve enquadramento sobre a Estónia

Situada no norte da Europa, a Estónia desenvolve-se ao longo da costa oriental do Mar Báltico, com uma área total pouco superior a 45 mil quilómetros quadrados. Com pouco mais de 1,3 milhões de habitantes, 1/3 da população vive na capital Tallinn.

(Fonte Imagem – Retirada do site - http://www.quadrodemedalhas.com/olimpiadas/estonia-jogos-olimpicos.htm)

Figura 16 - Mapa da Estónia

Com um percurso histórico marcado por diversas ocupações, primeiro da Dinamarca, depois da Suécia, a Estónia tem sido ao longo da sua história alvo de múltiplas disputas dada a sua privilegiada posição geográfica.

A Estónia tem diversas minorias, como é o caso da Russa com 25,6% da população, Ucraniana com 2,1%, Bielorussa com 1,3% e Finlandesas com 0,9%. As restantes minorias perfazem cerca de 2,2% do total da População de acordo com os censos realizado em 2000 (CIA - The World Factbook, 2012).

Tendo alcançado a independência em 1918 e mergulhado num período de alguma instabilidade política, a Estónia foi anexada pela Rússia em 1940 e unilateralmente incorporada como a décima sexta república da então União Soviética, fruto do *Tratado Molotov-Ribbentrop*[94]. Durante a Segunda Guerra Mundial de 1941 a 1944 foi reocupada pela Alemanha e posteriormente integrada na União Soviética.

Com o colapso da União Soviética**,** a Estónia conquistou a sua liberdade e afirmou-se como Estado independente em 1991, desde logo preparando a sua "*máquina de Estado"* para se afirmar como país independente e fora do alinhamento Russo.

A Estónia é um Estado moderno, membro da NATO e da União Europeia desde 2004, sendo um dos países que ocupa a linha da frente na implementação de serviços eletrónicos ao cidadão, onde mais de 70% da população entre os 16 e os 74 anos utiliza a internet, todas as escolas do país estão ligadas em rede e a maioria dispõem de serviços de ensino à distância,

94 Nota: tratado de não-agressão firmado entre a União Soviética e a Alemanha Nazi em 1939.

grande parte das cidades é servida por uma rede de acesso público à internet onde a taxa de penetração dos serviços de telecomunicações móveis é bastante elevada (Portal do Governo da Estónia, 2012).

O País dispõe de diversos serviços e iniciativas inovadoras na áreas das novas tecnologias, por exemplo, é possível pagar impostos via internet ou consultar a execução da despesa do Estado, ou mesmo votar nas eleições[95].

Aliado a estes serviços prestados pelo Estado, o país dispõe de uma rede de pagamentos eletrónicos sofisticada, baseados na rede móvel, e de um sistema bancário com uma rede de atendimento automática (ATM) que serve a totalidade do território nacional.

Nomes como o Hotmail, KaZaa ou Skype estão ligados à Estónia uma vez que os seus criadores e fundadores são de origem Estónia (Portal do Governo da Estónia, 2005).

De certa forma, estes nomes erguem-se como ícones inspiradores de uma sociedade moderna, inovadora, que procura nas novas tecnologias, um espaço de crescimento e de afirmação da sua nacionalidade.

A Estónia é um pais que, depois da sua independência e a partir de 1997, tem apostado fortemente na digitalização e desmaterialização dos seus processos, incentivando particulares e empresas, nomeadamente na indústria financeira a conduzirem os seus negócios para a internet, agilizando a sua economia com as novas tecnologias de informação e comunicação.

4.2. Os Acontecimentos em Tallinn

Passados 15 anos da sua independência da ex-União Soviética, o Governo da Estónia decidiu mudar de localização uma estátua erigida em homenagem aos soldados Russos mortos na Segunda Guerra Mundial, memorial, este, que ocupava desde 1947 um lugar de destaque no centro da capital Tallinn, sendo constituído por uma estátua de bronze e um túmulo onde jaziam vários corpos de soldados soviéticos mortos na Segunda Guerra Mundial.

Este monumento denominado de “Libertadores de Tallinn” seria, por decisão política de Abril de 2007, transladado para um cemitério militar na periferia da cidade.

95 Nota: como em 2005, em que se realizaram pela primeira vez eleições para o governo local através da Internet.

Figura 17 - Monumento "Libertadores de Tallinn"

(Fonte Imagem – Retirada da wikimedia - BronzeSoldier01 - http://es.wikipedia.org/wiki/Soldado_de_bronce_de_Tallin#mediaviewer/Archivo:BronzeSoldier01.jpg)

Embora esta decisão política não fosse inédita, uma vez que após a independência a maioria dos símbolos, legados na Estónia pela ex-União Soviética, tivessem sido gradualmente substituídos, proibidos ou relegados para planos menores, este por ser um dos mais emblemáticos, sendo inclusivamente lugar de romaria anual a 9 de Maio[96] e também por ser um dos últimos símbolos da ocupação russa, gerou uma avalanche de acontecimentos que rapidamente resvalaram das ruas de Tallinn para o ciberespaço.

Assim que a decisão foi conhecida e o governo tomou providências para desencadear a mudança, grupos afetos às minorias russas revoltaram-se, alguns milhares de manifestantes foram violentamente dispersados pela polícia, os distúrbios prolongaram-se durante a noite de 26 de Abril para 27 de Abril de 2007 fazendo um morto, dezenas de feridos e três centenas de detidos (Soeiro & Portas, 2007).

Poucas horas de hiato entre os protestos perpetrados nas ruas de Tallinn, somaram-se protestos pelo ciberespaço, que muito rapidamente se transformaram em ataques a alvos governamentais e a empresas e serviços de relevo.

96 Nota: dia que assinala a vitória sobre a Alemanha Nazi na Europa.

4.3. Os Acontecimentos no ciberespaço

Rapidamente a agitação das ruas de Tallinn se propagou ao ciberespaço, numa primeira fase, ainda no final do mês de Abril, começaram a circular, em diversos sites e blogues, pedidos de apoio e condenação para a atitude "provocatória" do governo da Estónia. Nesta fase, os pedidos foram realizados quer dentro das fronteiras da Estónia, supostamente atribuídos aos nacionalistas Russos, quer fora.

As salas de "*chat*" e os fóruns foram invadidos por conversas e tópicos relacionados com este assunto, instigando à ação e escalpelizando ao máximo o assunto, na sua maioria utilizando a língua russa. Também as páginas de internet dos principais órgãos de informação foram extraordinariamente consultadas, por uma comunidade crescente de "internautas" ávidos de informação e preocupados com o desenvolvimento dos acontecimentos.

No início de Maio a situação alterou-se, da instigação ao protesto contra os principais órgãos, instituições e empresas da Estónia. Começaram a ser divulgados em diversos sítios pela internet códigos fonte, que permitem de uma forma muito simples criar "guiões" e pequenas aplicações "*botnets*" para se realizarem ataques a alvos pré-identificados, na sua grande maioria trata-se de ataques destinados a criar tráfego anormal sobrecarregando serviços e servidores, impedindo assim o seu normal funcionamento, degradando o serviço e, na maioria das vezes em ataque coordenado, levando mesmo os servidores a pararem ou a entrarem em colapso. Estes ataques tiveram origem de várias partes do mundo, sendo procedentes também da Rússia.

A maioria destes ataques foram do tipo *DDOS-Distributed Denial of Service*. No total foram oficialmente registados pela Arbor Networks [97] cerca de 128 ataques, com a seguinte distribuição temporal e IP/sítio atacado:

97 Fonte: Arbor Networks, empresa especialista em segurança na internet, que disponibiliza um observatório mundial de incidentes assim como um reputado índice de ameaças na internet (http://atlas.arbor.net/) . Esta reputada empresa realizou um relatório especial sobre os acontecimento da Estónia, disponível para consulta em: http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/ Acedida em 4 de Janeiro de 2012

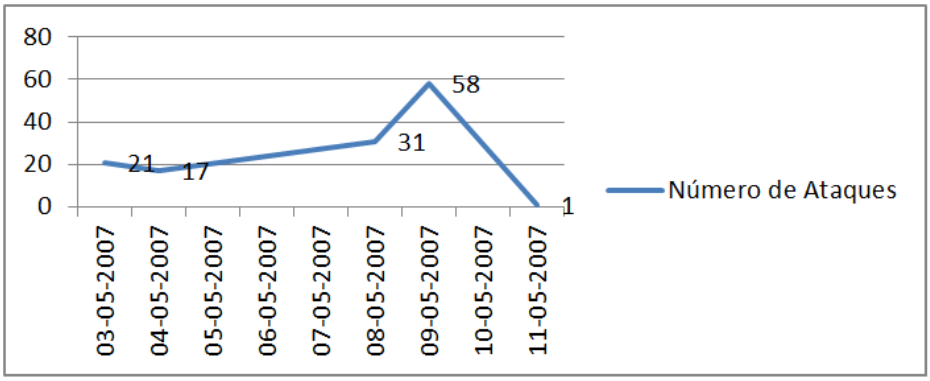


Figura 18 - Gráfico com a distribuição de Ataques por Data

(Fonte Imagem – Retirada da Arbor Networks - http://atlas.arbor.net/)

Os ataques registados tiveram uma duração de entre poucos minutos, aos mais longos com cerca de 10 horas. Na lista de alvos oficialmente registados pela Arbor Networks como atacados encontram-se os sites da internet da Polícia e do Ministério das Finanças com 35 ataques, respetivamente, o Portal do Governo o Site do Primeiro-ministro e o importante Portal do Estado do Cidadão com 36 ataques, seguidos do Parlamento com 7 ataques, Ministério da Agricultura com 6 e dos Ministérios do Ambiente e dos Assuntos Sociais com 2 ataques respetivamente.

A esta lista podem-se acrescentar ainda dificuldades em estabelecer ligações via internet, congestionamentos nas linhas telefónicas, dificuldades em realizar operações nas redes de multibanco, inacessibilidade aos serviços de HomeBanking, inacessibilidade aos principais serviços do estado e órgãos de comunicação social, alteração de conteúdos e fontes de informação on-line (Joshua, 2007).

Com o colapso de partes importantes do sistema, com algumas das infraestruturas criticas nacionais afetadas ou inoperantes, o Estado ficou parcialmente paralisado.

O Caso da Estónia é assim paradigmático da importância deste novo ambiente estratégico, temos pela primeira vez na história um alto representante de um Estado, Urmas Paet, ministro dos negócios estrangeiros da Estónia, qualificou o ataque de forma abrangente dizendo que "A Resposta da Rússia para a mudança de um memorial de guerra soviético é um "ataque" a toda a União Europeia "[98], esta afirmação vinda de um membro da NATO e da União Europeia, e muito embora se possa compreender a eventual manobra de defesa por detrás destas afirmações, poderia ter outra amplificação e ter levado a outro tipo de consequência, para além de um corte de relações diplomáticas entre os dois países, decretado pela Rússia, que

98 Fonte: BBC News (2007). - Russia accused of 'attack on EU. Referência de Tradução “Russia's response to the row over a Soviet war memorial is an "attack" on the whole European Union”; 2 de Maio. Acedida em 4 de Janeiro de 2012. Informação disponível para consulta em: http://news.bbc.co.uk/2/hi/europe/6614273.stm

sempre desmentiu o seu envolvimento nesta situação, poderia no limite provocar uma situação de Guerra, entre Estados.

Este exemplo serve como prova inequívoca de que se podem deduzir implicações e consequências concretas das ações realizadas, na Nova Pangeia, e que estas podem representar ameaças concretas para os Estados, e não apenas a entidades ou empresas privadas, como até aqui se faria limitadamente acreditar.

Este episódio vem destacar a importância deste novo contexto, e deu-lhe uma nova escala, amplificando o fenómeno a uma dimensão que se situa ao nível do Estado, atingindo recursos e infraestruturas críticas, que quando afetadas impactam não só o normal funcionamento das instituições, como acarretam consequências para os cidadãos, impedindo o acesso a serviços vitais e a recursos próprios.

Interessa pois tentar deduzir implicações lógicas e físicas para os ataques cibernéticos.

4.4. Implicações lógicas e físicas dos ataques cibernéticos

O General Loureiro dos Santos no seu livro "As Guerras que já aí estão e as que nos esperam se os Políticos não mudarem" define, como principais características deste novo ambiente estratégico, as seguintes:

- **Um contexto de permanente e obsessiva presença mediática;**
- **A possibilidade de comunicação em tempo real, aproximando dramaticamente a decisão da execução;**
- **A capacidade de motivação, praticamente sem limite espacial, através do apelo aos valores culturais;**
- **Um novo e ainda pouco explorado teatro de operações, a Internet;**
- **Um desenvolvimento científico-tecnológico em expansão exponencial;**
- **Sociedades avançadas muito complexas e vulneráveis;**
- **Novos *hubs* económicos de empresas que dominam as novas tecnologias;**
- **A globalização económica/financeira aliada ao impacte da tecnologia.**

Tendo como ponto de partida as características enunciadas, podemos traçar um quadro de ameaça alargada ao Estado, e à sua respetiva soberania.

Podemos percorrer o Processo Subversivo, segundo Garcia (2006), e recorrendo ao caso de estudo da Estónia, enquadrar as implicações lógicas e físicas dos ataques cibernéticos.

Assim**,** no período designado por pré-insurrecional encontramos 2 fases:

1ª Fase – Preparatória – O movimento focaliza a sua ação na organização, recrutamento e treino de elementos-chave, bem como selecionando e estabelecendo ligações a organizações legítimas no sentido de promover mecanismos de suporte ao movimento, atuando sempre em segredo. Nesta fase de incepção é estabelecida a estrutura celular clandestina de suporte com o objetivo de recolher informação estratégica[99] e estabelecer um comando de operações.

Após os primeiros ataques à Estónia, multiplicaram-se os pedidos de insurreição em blogues e fóruns, apelando à força e ao ataque físico e digital contra o governo e suas principais instituições.

2ª Fase – Agitação – O movimento promove a infiltração de elementos em lugares-chave do Estado. Entra em funcionamento a propaganda, no sentido de explorar matérias populistas e aumentar simpatias para a causa, pondo em causa os poderes instituídos.

Esta é uma das principais utilidades deste novo contexto, uma vez que a sua utilização maximiza e facilita o contacto, tendo uma força mobilizadora até aqui pouco compreendida. Em poucas horas, das centenas de manifestantes nas ruas de Tallinn assistem-se a dezenas de

99 Nota: no sentido de strategic intelligence.

milhares de mensagens trocadas na Internet, os fóruns e blogues foram atulhados de vozes de descontentamento, os ataques, começaram a desenhar-se.

Entramos no período designado por insurrecional:

3ª Fase – Armada – O movimento aciona medidas desafiantes à autoridade do poder instituído. Estas ações incluem assassinatos, sabotagem, ataques indiscriminados e outras atividades subversivas como disrupção de redes e sistemas de informação. Esta fase (de terrorismo e/ou guerrilha) tem por objetivo desacreditar o poder e as autoridades instituídas pondo em causa a sua legitimidade para o exercício desse poder.

No caso da Estónia, as fases 4 e 5[100] não foram aplicadas, tendo a sua ação ficado pela 3ª Fase dita Armada, com os tumultos a serem repelidos nas ruas por agentes policiais, que tentam controlar os manifestantes tentando repor a ordem pública.

O potencial de subversão deste novo ambiente estratégico é evidente, a importância deste episódio, para além de ter sido o primeiro na história em que um Estado objetivamente acusa outro de ofensivas/ataques cibernéticos qualificados como atos de guerra, expõe uma série de outras questões relacionadas não só com a segurança do próprio Estado como, também, o direito de resposta que eventualmente lhe assiste, e como o mesmo deve lidar com mais esta nova forma de subversão.

Se anteriormente a esta situação vivida na Estónia as ameaças cibernéticas se podiam qualificar do ponto de vista do Estado na sua grande maioria como dentro de um conceito mais abrangente ou de *Information warfare* ou como atos de *Cyber Terrorismo*, após os ataques verificados e depois da reação do governo da Estónia, poderemos falar substantivamente de Guerra Cibernética, e de tentativa de subversão do Estado utilizando este novo ambiente estratégico.

O ciberespaço tornou-se no quinto domínio da guerra, depois da terra, mar, ar e espaço, disponibilizando um cenário de operações iminentemente novo e por explorar.

As novas armas deste teatro de operações são pouco conhecidas, sendo que os seus efeitos podem ser antecipados pelos episódios, já frisados, mas podem ser amplificados na medida em que cada vez a ligação entre acontecimentos ocorridos no Ciber Espaço se podem propagar a outros sistemas.

100 Nota: Discrição da 4ª e 5ª Fase - 4ª Fase – Estado Insurrecional ou Revolucionário – o movimento tem já uma capacidade organizativa formal apreciável comportando-se do ponto de vista da luta armada como um exército regular. A situação assume contornos de guerra civil e os insurgentes controlam e administram parcelas do território. Este foi durante largos anos a situação vivida em Angola, pós-independência.
5ª Fase – Final – É atingido o objetivo do movimento. As autoridades instituídas não são já capazes de administrar o território e assiste-se à tomada do poder. As Forças Armadas estão destruídas ou são incorporadas nas forças ex-revolucionárias. Assiste-se progressivamente ao reconhecimento internacional da nova autoridade.

Esta nova forma de subversão ou de guerra será não apenas mais uma "ferramenta", instrumento de defesa ou de ataque, mas também uma forma revolucionariamente nova de inter-relacionar teatros de operações e campos de batalha, acrescentado de forma disruptiva um elemento novo, que se distancia de todos os outros, por dois fatores fundamentais, é virtual, e até agora integralmente concebido pelo homem.

Sendo que, em matéria de subversão, as bandeiras do descontentamento e muitas das ações contra o Estado, que acompanham o processo subversivo, serão muito provavelmente guisadas ao teclado de um computador, onde serão lançados sob as mais diversas forças e intensidades.

5. CAPÍTULO - CONCLUSÕES

Na presente dissertação "**Nova Pangeia – Ameaças vindas do Ciberespaço**" realizou-se em primeiro lugar uma caracterização sistémica da Nova Pangeia. Dessa tarefa resulta a fundamentação do conceito objeto deste trabalho, deduzindo-se que Nova Pangeia, toma como ponto de partida a teoria da "Deriva Continental" de Alfred Wegener (1975, p.88), evoluindo com base nos conceitos de "Aldeia Global" de Marshall McLuhan (1962), "Pangeia 2" de Wolf Schäfer (2003, p.76), "Terceira Revolução Industrial" de Jeremy Rifkin (2014) e no conceito de Ciberespaço proposto por Gibson (1983) no livro Neuromancer, dando origem assim ao conceito de base deste trabalho: "**Nova Pangeia": Pan (todos) + Gaia (terra) + Ciberespaço: sistema organizado em rede, com causalidade interconetiva.**

Deduzido o conceito, aprofundou-se a sua caracterização, do ponto de vista da sua genética com a discrição das suas duas principais componentes sistémicas. Uma denominada "Sistema Físico", centrada fundamentalmente ao nível da infraestrutura, donde se destaca a Internet, rede mais usada e disseminada em termos Globais, e para a qual foram apresentados os seus principais componentes teóricos, visando a compreensão do seu funcionamento, em alto nível, e permitindo o entendimento da sua arquitetura e principais funções, transporte e ligação/conexão entre pontos/sistemas.

A outra componente designada "Meio Lógico", e que diz respeito às aplicações ou códigos que a rede transporta, apresentou-se recorrendo a um modelo que árbitra e regulamenta a troca de informação e dados entre sistemas, nomeadamente hardware e software, interfaces de acesso à rede e suas funcionalidades.

Cumpre-se assim o primeiro objetivo proposto por este trabalho**: Realizar a caracterização sistémica deste novo Sistema - "Nova Pangeia"** – Concluindo-se pela possibilidade de existência deste novo espaço/sistema, e dando-se por verificados os seus princípios básicos de funcionamento, componentes e estruturas fundamentais.

Seguidamente o trabalho desenvolveu-se com a identificação dos padrões básicos dos ataques Cibernéticos. Recorreu-se ao modelo descrito por Janczewski (2007, Cpt. XV), verificando-se que em larga medida, estes ataques obedecem a um padrão básico de ataque faseado, independentemente da sua complexidade, podem ser enquadráveis em termos de manobra subversiva ou crime tradicional. A proposta deste autor desenvolve-se basicamente em 5 fases distintas (Reconhecimento das Vítimas/Alvos, Penetração, Identificação de capacidades, Produção do Dano, Eliminação da Prova).

Seguidamente apresentaram-se os tipos de ataque e veículos mais utilizados. Comprovando-se que, esses ataques podem ser desencadeados recorrendo aos mais diversos tipos de técnicas, podendo ser "ubíquos" em termos do tipo de transporte e acesso utilizado e recursos

a utilizar e alvos a atingir. Sendo que desta forma o seu potencial de dano não se limita a esses fatores, o que em termos táticos e estratégicos dificulta e torna mais sofisticadas, as operações de defesa ou mitigação de danos ou de ataque de retaliação.

Retira-se assim um primeiro **contributo para os Estudos Estratégicos, e para a área da Segurança no Ciberespaço**, também um dos objetivos deste trabalho, na medida em que estamos perante um sistema complexo, capaz de produzir ameaças variadas, recorrendo aos mais diversos tipos de técnicas e veículos. Sendo que as manobras de defesa e ataque implicam um grau de especialização concreto e uma preparação específica e própria para o sistema apresentado.

Com a verificação da correlação entre ataques cibernéticos e convencionais, responde-se afirmativamente a uma das questões de partida colocadas neste trabalho **– Será possível Correlacionar Ataques Cibernéticos e Convencionais?**

Fica pela investigação demonstrado que a resposta é afirmativa, sendo que os ataques cibernéticos, surgem como os convencionais tendo como base uma estratégia, a sua preparação desenvolvida recorrendo naturalmente a conhecimentos específicos, que se ajustam tendo em conta cenários ou operações a desenvolver e os objetivos a atingir. Podendo-se estabelecer uma relação entre dois campos fundamentais e comuns, ou seja, a ação ofensiva e ação defensiva.

Para isso estabelece-se um valor para qualquer elemento do recurso informação, podendo este constituir-se como alvo daquele que procura retirá-la ao seu possuidor, com o objetivo de ganhar uma vantagem nesse ou noutro campo. Sendo neste conflito a informação um ganho/perda típica do jogo, conforme Bispo (2001).

Fica também claro que o ato de guerra se estende para além da guerra de informação, abrangendo outras dimensões, como a Guerra económica, eletrónica, psicológica e Covert cyberwarfare num cenário que para a Estratégia, e nomeadamente para a militar e forças de segurança, implica uma abertura de considerações muito maior e um esforço de entendimento de fenómenos mais alargado e suas respetivas correlações, como foram sendo evidenciadas ao longo deste trabalho.

Surgindo assim a segunda questão de investigação proposta neste trabalho: **Existem interdependências entre Infraestruturas Críticas Nacionais e a Nova Pangeia?**

A verificação desta questão iniciou-se com a definição para infraestrutura crítica Nacional (ICN) e infraestrutura crítica europeia (ICE), seguidamente avançou-se com a inventariação dessas infraestruturas críticas (IC) tendo-se optado por recorrer à classificação de (IC) segundo

a Homeland Security [101] e para cada um dos 16 sectores elencados**,** foi realizada uma análise agrupada e organizada por forma a identificar as principais vulnerabilidades e vias de ataque, tentando assim verificar a existência de interdependências, assim como de consequências, para a Segurança do Estado, sempre numa perspetiva relacionada com a Nova Pangeia.

Fica demonstrado que essas interdependências entre ICN e a Nova Pangeia existem, embora variando de intensidade consoante o setor e IC, ficando também patente a capacidade de estas serem afetadas por fenómenos provimentos da Nova Pangeia e em especial por ataques provimentos do Ciberespaço. As IC enquanto suportes base do funcionamento das sociedades modernas e dos Estados em si, e por intermédio dos relatos de situações já ocorridas e neste trabalho analisadas e apresentadas, demonstra-se que caso estas infraestruturas sejam afetadas ou colapsadas, Estados e Indivíduos podem sofrer consequências graves, que podem não ficar apenas confinadas a percas materiais, desvendando-se assim a importância e influencia maior que este novo sistema representa para as sociedades modernas e para a Segurança Nacional, sendo que os Estudos Estratégicos devem a esta matéria dispensar uma atenção específica com o objetivo de construírem um conjunto de respostas, que valorize estes cenários e permitam criar medidas de salvaguarda adequadas para estas situações.

Ficam também ao longo deste trabalho evidenciadas as **novas ameaças e vulnerabilidades provenientes do ciberespaço**, profusamente descritas pela análise das interdependências entre Infraestruturas Críticas Nacionais e a Nova Pangeia e pela **Avaliação estratégica de risco quer para a "Nova Pangeia" e sistemas a ela interconectadas** objetivos também centrais desta investigação.

Assim verificou-se o seu impacto, na sociedade e nos indivíduos avaliando as suas forças, fraquezas, ameaças e oportunidades. Concluindo-se que existe um movimento Global que facilitou e estimulou a ligação entre povos, para além da criação de vastas comunidades on-line, gerando oportunidades diversas que contudo encerram ameaças concretas quer para os indivíduos, quer para os Estados quer inclusivamente às infraestruturas da **Nova Pangeia**, que por sua vez os inter-influenciam, podendo ocorrer o seu colapso e consequentemente acarreando risco de variada ordem e natureza para os indivíduos e para os Estados, conforme fica demonstrado.

Por outro lado, fica patente, nos sete cenários apresentados que esses riscos e ameaças são de grandeza bidirecional e unidirecional, sendo evidente a sua capacidade de produção de dano, prejuízo ou colapso de variada ordem e natureza. Conclui-se pois que os cenários apresentados podem abranger diversas circunstâncias (diversos nós) e a sua perigosidade

101 Nota: Departamento de Segurança Interna dos EUA segundo a Diretiva Presidencial 21 (PPD-21): Segurança Infraestrutura crítica e Resiliência avanços de uma política nacional para fortalecer e manter a segurança, funcionamento e infraestrutura crítica resiliente. Mais informação disponível para consulta em: http://www.dhs.gov/critical-infrastructure-sectors

para o sistema é naturalmente maior tendo mais impacto em termos de risco e consequentemente capacidade de abalar pilares fundamentais da nossa sociedade.

Esta situação fica ainda mais clara com o **Estudo de Caso da Estónia**, onde claramente são demostrados os impactos que estas ameaças podem traduzir numa situação real e seu impacto direto quer para os cidadãos quer para o Estado em si.

Os Estudos Estratégicos têm assim de refletir sobre a importância e dimensão deste novo espaço, se na América do Norte a taxa de penetração da Internet se encontra na casa dos 78,8%, seguida da Oceânia com 67,5% e Europa com 61.3% (Internet World Usage Statistics, 2001 – 2012), geografias onde o processo de "internetização" decorre a um ritmo mais acelerado, onde a cada dia estes indicadores tem tendência a crescer. Estes números parecem confirmar a colonização, em massa, deste novo território.

É assim evidente a importância da **Nova Pangeia**, embora seja um espaço alargado de convivência entre antagonismos, a dependência das sociedades modernas dela, é acima de tudo reveladora de como estamos a construir o nosso desenvolvimento e de como dele estamos dependentes.

Conclui-se pois que a **Nova Pangeia** forma um novo sistema, que configura um importante ambiente estratégico, cuja importância está muito para além da sua lógica sistémica, não se limitando a influenciar e a produzir efeitos em si, mas também em outros sistemas quer físicos quer lógicos, abarcando diversas dimensões e ultrapassando fronteiras e barreiras físicas e lógicas, formando um contínuo quase planetário, com capacidade de afetar positivamente ou negativamente em grande escala o mundo onde vivemos e a realidade que conhecemos.

Assim os Estudos Estratégicos e o processo de tomada de decisão Estratégica devem levar em consideração todas estas novas variáveis, traduzidas em termos de riscos e ameaças apresentadas, incluído no seu pensamento e doutrina este sistema específico e para ele criando um conjunto de respostas, que permita garantir a segurança dos Cidadãos dos Estados e dos seus interesses de forma eficaz e na mesma medida em que em outros sistemas ditos tradicionais lhes é garantida a Segurança.

A Guerra dos Bits e Bytes versus a Guerra das Balas e dos Canhões será certamente o paradigma da guerra moderna, e com toda a certeza, um dos denominadores comuns dos conflitos doravante.

6. BIBLIOGRAFIA

Abraham D. Sofaer & Seymour E. Goodman (2001).The Transnational Dimension of Cyber Crime and Terrorism - The Civil Aviation Analogy: Part II: Cyber Terrorism and Civil Aviation contribute Whiteman. Stanford. H.H. Stanford University. Hoover Institution Press.

Arquilla, Jonh & Ronfeldt Dorothy (2001). Networks and Netwars: The Future of Terror, Crime, and Militancy. Capítulo 8, pag. EUA. 220. National Defense Research Institute – RAND.

Barrento, António (2010). Da Estratégia. Pag.246- 300.Parede. Tribuna da História.

Beaufre, André (2004). Introdução à Estratégia. 1ª Edição. Lisboa. Edições Sílabo.

Bernard Huygh, François (2008).Maîtres du faire croire : De la propagande à l'influence. França Vuibert.

Bispo, Ten. Gen. Pil. Antonio (2001) A Sociedade de Informação e a Segurança Nacional. Lisboa Estratégia artigo. Volume XIII, pag. 91. ISCSP.

Correia, Major-General Pedro de Pezarat (2004). Teoria do Combate - Carl von Clausewitz Estudo introdutório e Notas. Lisboa Pag. 35. Edições Sílabo.

Decreto-lei nº 62/2011 de 9 de Maio. Diário da República N.º 891/11 - I Série. Ministério da Defesa Nacional. Lisboa.

Falcone, Rino. Singh & Munindar. Tan, Yao-Hua (2001).Trust in Cyber-societies- Integrating the Human and Artificial Perspectives. Berlim.Springer.

Garcia, Francisco (2006). O Fenómeno Subversivo na Atualidade - Contributos para o seu Estudo. Lisboa Revista. "Nação Defesa" nº 114 – 3ª série – Verão

Geers, Kenneth (2011). Strategic Cyber Security. NATO Cooperative Cyber Defence Centre of Excellence. NATO. Estonia.

Georgia Tech Information Security Center (GTISC). The Georgia Tech Research Institute (GTRI). (2013). Georgia Tech Emerging Cyber Threats Report for 2013. Georgia Tech Cyber Security Summit. Georgia.

H. Moor, James & Ward Bynum, Terrell. (2003).CyberPhilosophy: The Intersection of Philosophy and Computing. I edição. EUA. Wiley-Blackwell.; Janeiro.

Halabi, Sam, McPherson, Danny (2000).Internet Routing Architectures. Segunda Edição. EUA. Cisco Press EUA.

Hough, Peter (2004). Understanding Global Security. Londres. Routledge.

Jabbour, Kamal (2010).CyberVision and Cyber Force Development. Vol. 4, No. 1, Pag 64 -70. EUA Strategic Studies Quarterly.

Janczewski, Lech J. (Author, Editor), M. Colarik, Andrew (Editor) (2007). Cyber Warfare and Cyber Terrorism. 1 Edição .EUA. IGI Global.

Joshua, Davis (2007). Hackers Take Down the Most Wired Country in Europe. EUA. Artigo Número 15.09. WIRED MAGAZINE.

Kenneth, J. Knapp (2009). Cyber Security and Global Information Assurance: Threat Analysis and Response Solutions. 1ª Edição. U.S. Air Force Academy. EUA. Information Science Reference.

Lara, António de Sousa (2005). Ciência Política. Estudo da Ordem e da Subversão. 3ª Edição. Lisboa. ISCSP.

Lech J. Janczewski & Andrew M. Colarik (2008). Cyber Warfare and Cyber Terrorism. Information science reference. New York. Hershey.

Levitt, Theodore (1983). The globalization of markets. Volume 61, nº3, Maio-Junho, pag. 92 a 102. EUA. Harvarad Business Review

Marques, Contra-Almirante António Gameiro (2010). Conferência 17/3. Conferencia. Segurança no Ciberespaço. ISCSP a 17 de Maio de 2010.

McLuhan, Marshall (1962). The Gutenberg Galaxy: The Making of Typographic Man. University of Toronto. Canada. Press - Social Science.

Monteiro, Edmundo & Boavida Fernando (2011).Engenharia de Redes Informáticas. 10ª Edição. Lisboa. FCA - Editora Informática.

Nakashima, Ellen (2013). Confidential report lists U.S. weapons system designs compromised by Chinese cyberspies. Artigo. EUA. Washington Post; 27 de Maio.

Nelson, Major Bill, Choi, Major Rodney, Major Michael Lacobucci, Mitchell, Major Mark, Gagnon, Captain Greg (1999).Cyberterror Prospects and Implications. White Paper. Prepared for: Defense Intelligence Agency Office for Counterterrorism Analysis. (TWC-1).Monterey, EUA. Center for the Study of Terrorism and Irregular Warfare.

Obama. President Barack (2009).Internatitional Strategy for Cyberspace - Prosperity, Security, and Openness in a Networked World. EUA. The White House. Washington.

Ohmae, Kenichi (1995). Putting Glogal logic first. Volume 73, nº1. EUA. Harvard Business Review.

Rebelo de Sousa, António (2004). Da Teoria da Relatividade Económica Aplicada à Economia Internacional e às Políticas de Cooperação. Lisboa. Universidade Lusíada.

Ribeiro, Almirante António Silva (2009). Teoria Geral da Estratégia: O essencial ao processo estratégico. Lisboa. Almedina.

Rifkin, Jeremy (2014). A Terceira Revolução Industrial. Lisboa. Bertrand Editora.

Santos, A.R. (1999). Metodologia científica: a construção do conhecimento. Brasil. DP & A.

Santos, General José Alberto Loureiro dos (2009). As Guerras Que Já Aí Estão e as Que nos Esperam se os Políticos Não Mudarem - Reflexões sobre Estratégia. Vol. VI. Lisboa. Europa-America.

Sharma, Amit (2010). Cyber Wars: A Paradigm Shift from Means to Ends. Institute for System Studies and Analysis (I.S.S.A). India. Defence Research and Development Organization (D.R.D.O) Ministry of Defence.

Soeiro, Renato, Portas, Miguel (2007). Artigo. Estónia - A luta pelos Símbolos. Lisboa. Jornal Global. Maio.

Stiglitz, Joseph E. (2007) Tornar Eficaz a Globalização. Pag. 337-340. Lisboa. Edições Asa.

Tzu, Sun (2006). A Arte da Guerra. Lisboa. Edições Silabo.

UK Office of Cyber Security, UK Cyber Security Operations Centre. (2009) Presented to Parliament by the Prime Minister Gordon Brown, by Command of Her Majesty - Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space. Londres. Crown.

Wegener, Alfred (1929). The Origin of Continents and Oceans. (4th edition). Translated from the Fourth Revised German Edition by John Biram with an Introduction by B. C. King. London. Methuen and Co.

Wegener, Alfred (1975).The Hypothesis of Continental Drift. pp 88-97.EUA. Scientific American.

World Usage Statistics (2001 – 2012). World Internet usage and Population Miniwatts Marketing Group. EUA.

Yin, Robert K (2009). Estudo de caso: planeamento e métodos. 2ª Edição. Bookman. Londres.

Yin, Robert K. (2009). Case Study Research - Design and Methods. 4ª Edição. Londres.SAGE.

Bibliografia consultada e disponível on-line:

Agência Noticiosa da Coreia Yonhap (2011).Seoul to build traffic control tower resistant to cyber-attacks. Acedida em 13 de Novembro de 2012. Informação disponível para consulta em:

http://english.yonhapnews.co.kr/national/2011/07/20/60/0302000000AEN20110720002000315F.HTML

AJAP - Associação dos Jovens Agricultores de Portugal. Acedida em 12 de Abril de 2014. Mais informação disponível para consulta em:

http://agrinov.ajap.pt/agriprecisao.asp

Arbor Networks (2007). Relatório especial sobre os acontecimentos da Estónia. Acedida em 4 de Janeiro de 2012. Informação Disponível para consulta em:

http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

Armerding, Taylor (2013).Hackers say coming air traffic control system lets them hijack planes. CSOonline.com. 13 Janeiro. Acedida em 16 de Fevereiro de 2014. Informação disponível para consulta em:

http://www.csoonline.com/article/726281/hackers-say-coming-air-traffic-control-system-lets-them-hijack-planes

Ashford, Warwick (2012).Cybercrime a growing threat to financial sector, says PwC. CYBERSECURITY. Março. PWC. Acedida em 16 de Novembro de 2013. Informação disponível para consulta em:

http://www.computerweekly.com/news/2240147503/Cybercrime-a-growing-threat-to-financial-sector-says-PwC

BBC News (2007).Russia accused of 'attack on EU. Referência de Tradução “Russia's response to the row over a Soviet war memorial is an "attack" on the whole European Union”; 2 de Maio. Acedida em 4 de Janeiro de 2012. Informação disponível para consulta em:

http://news.bbc.co.uk/2/hi/europe/6614273.stm

C. White, Martha (2012). Identity Theft - Visa, MasterCard Suffered ‘Massive’ Data Breach”. Revista Time. Março. Acedida em 15 de Novembro de 2013. Informação disponível para consulta em:

http://business.time.com/2012/03/30/visa-mastercard-suffered-massive-data-breach/#ixzz2H0bBGEkg.

CCDCOE (2012). Cyber Attacks Against Georgia: Legal Lessons Identified. Acedido em 17 de Fevereiro de 2014. Disponível para consulta on-line em:

http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf

CIA - The World Factbook. Acedida em Janeiro de 2012. Informação disponível para consulta em:

https://www.cia.gov/library/publications/the-world-factbook/geos/en.html

Cloherty, Jack (2012).Virtual Terrorism: Al Qaeda Video Calls for 'Electronic Jihad. ABC News. EUA. Maio. Acedida em 15 de Novembro de 2013. Informação disponível para consulta em:

http://abcnews.go.com/Politics/cyber-terrorism-al-qaeda-video-calls-electronic-jihad/story?id=16407875#.UOeWCySp3up

Computerworld (2011). Segurança – Maiores Ciberataques 2011. Acedido em 17 de Fevereiro de 2014. Disponível para consulta on-line em:

http://computerworld.uol.com.br/seguranca/2011/12/28/seguranca-maiores-ciberataques-de-2011/

Danchev, Dancho (2008). Coordinated Russia vs Georgia cyber-attack in progress. Zero Day. Acedida em 14 Março de 2012. Informação disponível para consulta em:

http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670

Departamento de Segurança Interna dos EUA segundo a Diretiva Presidencial 21 (PPD-21): Segurança Infraestrutura crítica e Resiliência avanços de uma política nacional para fortalecer e manter a segurança, funcionamento e infraestrutura crítica resiliente. Acedido em 18 de Março de 2013. Mais informação disponível para consulta em:

http://www.dhs.gov/critical-infrastructure-sectors

Espiner,Tom (2008). CIA: Cyberattack caused multiple-city blackout. CNET. Janeiro. Acedida em 13 de Novembro de 2013. Informação disponível para consulta em:

http://news.cnet.com/2100-7349_3-6227090.html

FAD - Food and Agriculture Sector-Specific Plan - An Annex to the National Infrastructure Protection Plan. Acedida em 6 de Abril de 2014. Mais informação disponível para consulta em:

http://www.fda.gov/downloads/Food/FoodDefense/UCM243043.pdf

FBI (2013).The Internet Crime Complaint Center (IC3). EUA. Acedido em 16 de Fevereiro de 2014. Relatório disponível para consulta em:

http://www.ic3.gov/media/annualreport/2013_IC3Report.pdf

Figueiredo Lopes (2012).Falta programa nacional de proteção de infraestruturas. Lisboa. Agencia Lusa. (2012). Acedido em 16 de Fevereiro de 2013, informação disponível para consulta em:

http://www.dn.pt/inicio/portugal/interior.aspx?content_id=2327004

Figueiredo Lopes (2013). Obama acusa China de apoiar ataques informáticos. Publicado em 03-13. Lisboa. Jornal de Notícias. Acedido em 6 de Maio de 2013, disponível para consulta em:

http://www.jn.pt/PaginaInicial/Mundo/Interior.aspx?content_id=3105261

Finkle, Jim (2011).U.S. probes cyber attack on water system. Reuters. Novembro de 2011. Acedida em 16 de Fevereiro de 2013. Informação disponível para consulta:

http://www.reuters.com/article/2011/11/21/us-cybersecurity-attack-idUSTRE7AH2C320111121

Gibson, William (1983). – Neuromancer. Vancouver. pag. 31, acedido em 8 de março de 2013, disponível para consulta em:

http://www.hugocarrion.com/index_archivos/Docs/A_neuromancer.pdf

Giurgiu, Anca (2013).When did all our eating habits become so transport intensive?. London Remade. Julho. Acedida em 9 de Janeiro de 2014. Informação disponível para consulta em:

http://londonremade.com/when-have-all-our-eating-habits-become-so-transport-intensive/

Global Geopolitics & Political Economy (2010). Acedida em 18 de Fevereiro 2013. Informação disponível para consulta em:

http://globalgeopolitics.net/wordpress/2010/12/01/wikileaks-implications-of-leakage-of-us-diplomatic-cables/

Global Research & Analysis Team (GReAT), (2013). Laboratórios Kaspersky. 15 de Novembro de 2013. Acedida 8 de março de 2014. Informação disponível para consulta em:

http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies

Gonçalves, C.P & Madeira, M.O (2009) A Systems Theoretical Formal Logic for Category Theory". Acedida em 8 de Novembro de 2012. Informação disponível para consulta em:

http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396841

Government Accountability Office (GAO). Department of Homeland Security's (DHS's).Role in Critical Infrastructure Protection (CIP) Cybersecurity. GAO-05-434 (Washington, D.C.: May, 2005). Acedida em 13 de Março de 2913.Mais informação disponível em:

http://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions

Greenberg, Andy (2011). LulzSec Hackers Deface The Sun Newspaper To Declare Rupert Murdoch Dead, Claim Stolen Emails. Revista Forbes. 2011. Acedida em 15 de Novembro de 2013.Informação disponível para consulta em:

http://www.forbes.com/sites/andygreenberg/2011/07/18/anonymous-hackers-hack-the-sun-newspaper-to-declare-murdoch-dead-claim-stolen-emails/

Hayashi, Chiemi. Gleicher, David. Ramseger, Florian. Campbell, Karen. Soo, Amey. Tonkin, Samantha. Wright, Andrew. Stefaner, Moritz (2012). Global Risks 2012 – Seventh Edition, Switzerland. World Economic Forum. EUA. Acedido em 6 de março de 2013. Disponível para consulta em:

http://www.weforum.org/reports/global-risks-2012-seventh-edition.

Homeland Security - Departamento de Segurança Interna dos EUA (2013). Informação acedidos em 6 de Abril de 2014. Raiz da informação disponível para consulta em:

http://www.dhs.gov/critical-infrastructure-sectors

Diversos documentos, disponíveis para consulta em:

Chemical Sector – http://www.dhs.gov/chemical-sector

Commercial Facilities Sector - http://www.dhs.gov/commercial-facilities

Communications Sector - http://www.dhs.gov/communications-sector

Critical Manufacturing Sector - http://www.dhs.gov/critical-manufacturing-sector

Dams Sector - http://www.dhs.gov/dams-sector

Defense Industrial Base Sector - http://www.dhs.gov/defense-industrial-base-sector

Emergency Services Sector - http://www.dhs.gov/emergency-services-sector

Energy Sector Overview - http://www.dhs.gov/energy-sector

Financial Services Sector - http://www.dhs.gov/financial-services-sector

Food and Agriculture Sector - http://www.dhs.gov/food-and-agriculture-sector

Government Facilities Sector - http://www.dhs.gov/government-facilities-sector

Healthcare and Public Health Sector - http://www.dhs.gov/healthcare-and-public-health-sector

Nuclear Reactors, Materials, and Waste Sector - http://www.dhs.gov/nuclear-reactors-materials-and-waste-sector

Information Technology Sector - http://www.dhs.gov/information-technology-sector

Transportation Systems Sector - http://www.dhs.gov/transportation-systems-sector

Water and Wastewater Systems Sector - http://www.dhs.gov/water-and-wastewater-systems-sector

IBM - Internet Security Systems.EUA. Acedido em 16 de Fevereiro de 2012. Definição disponível para consulta em:

http://www.iss.net/security_center/advice/Underground/Hacking/default.htm

IBM Institute for Business Value "Smarter cities for smarter growth". Acedida em 6 de Abril de 2014.Mais informação disponível em:

http://www.ibm.com/smarterplanet/us/en/smarter_cities/solutions/planning_mgt_solutions/index.html?lnk=cities_systems#solutions_public_safety

IBM Smarter Cities. Acedida em 6 de Abril de 2014. Mais informação disponível em:

http://www.ibm.com/smarterplanet/us/en/smarter_cities/overview/

Information Age (2012). Can satellites be hacked?. Information Age magazine. 29 de Maio. Acedida em 7 de Abril de 2014. Informação disponível para consulta em:

http://www.information-age.com/technology/security/2105738/can-satellites-be-hacked

Information Sciences Institute University of Southern California (1981). - TRANSMISSION CONTROL PROTOCOL DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION. RFC:793. Setembro. Acedida em Novembro de 2012, disponível em:

http://www.ietf.org/rfc/rfc793.txt

Internet World Stats. Mobile Internet - Mobile Phones and Smart Mobile Phones. Acedida em 10 de Abril de 2014.Informação disponível para consulta em:

http://www.internetworldstats.com/mobile.htm

Joshua Davis (2007).Hackers Take Down the Most Wired Country in Europe. WIRED MAGAZINE, número 15.09 de 21-08. Acedida em 6 de Janeiro de 2012 Disponível também para consulta em:

http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all

King, Rachael (2013).DHS Report: Energy Sector Now a Bigger Target for Cyber Attackers. CIO Jornal. Junho. Acedido em 18 de Abril de 2014. Mais informação e disponível para consulta em:

http://blogs.wsj.com/cio/2013/06/28/dhs-report-energy-sector-now-a-bigger-target-for-cyber-attackers/

Microsoft (2011).Vírus informáticos: descrição, prevenção e recuperação. Artigo: 129972 - Fevereiro - Revisão: 2.1. Acedido em 7 de Novembro de 2012 disponível em:

http://support.microsoft.com/kb/129972/pt

N.Runs Professionals - Security Research Team (2013). Abril Acedida em 17 de Fevereiro de 2014. Apresentação disponível para consulta em:

http://conference.hitb.org/hitbsecconf2013ams/materials/D1T1%20-%20Hugo%20Teso%20-%20Aircraft%20Hacking%20-%20Practical%20Aero%20Series.pdf

Paganini, Pierluigi (2013). Hacking Satellites … Look Up to the Sky. InfoSec Institute. Setembro de 2013. Acedida em 20 de Abril de 2014. Informação disponível para consulta em:

http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/

Pasquali, Valentina (2012).International Reserves of Countries Worldwide. Global Finance. Dezembro. Acedida em 18 de Novembro de 2013. Informação disponível para consulta em:

http://www.gfmag.com/component/content/article/119-economic-data/12374-international-reserves-by-country.html#axzz2l2UwG7nx

Portal do Governo da Estónia (2005). - Estonia – the homeland of Kazaa, Skype and Hotmail, Março. Acedida em 4 de Janeiro de 2012.Disponível para consulta em:

http://web-static.vm.ee/static/failid/378/IT_achievements2.pdf

Portal do Governo da Estónia. Acedida em 4 de Janeiro de 2012. Informação disponível para consulta em:

http://veebik.vm.ee/estonia/kat_175/pea_175/1163.html

Presidente do Concelho Nacional de Investigação e Desenvolvimento do Ministério das Ciências Israelitas citado por Ronen, Gil; "Syrian Cyber-Attack on Haifa Water System"; Israel National News; Maio de 2011. Acedida em 6 de Abril de 2014. Mais Informação disponível para consulta em:

http://www.israelnationalnews.com/News/News.aspx/168306#.UqcHztTuP4g

Price Waterhouse Coopers LLP (2013). As cyber attacks hit financial firms, threat analysis and warning grow in importance. Janeiro. Acedida em 16 de Novembro de 2013.Informação disponível para consulta em:

http://emarketing.pwc.com/reaction/images/Cyber.Financial.Zoomlens.R&Q.Approved_FINAL.pdf

Prince, Brian (2011) - Coordinated Cyber Attacks Hit Chemical and Defense Firms. Security Week. Outubro. Acedida em 6 de Janeiro de 2014. Informação disponível para consulta em:

http://www.securityweek.com/coordinated-cyber-attacks-hit-chemical-and-defense-firms

Schäfer, Wolf (2003).The New Global History Toward a Narrative for Pangaea Two. State University of New York at Stony Brook, Department of History. EUA – Acedida em 16 de Maio de 2014. Disponível para consulta em:

http://www.ebooksmagz.com/pdf/the-new-global-history-toward-a-narrative-for-pangaea-two-200456.pdf

Soeiro, Renato & Portas, Miguel (2007). Estónia: Luta pelos seus símbolos. Publicado em: Global em Maio de 2007. Acedida em 4 de Janeiro de 2012. Disponível para consulta em:

http://renatosoeiro.blogspot.com/2008/04/estnia-luta-pelos-smbolos.html

Stamford, Conn (2007). Gartner Survey Shows Phishing Attacks Escalated in 2007; More than $3 Billion Lost to These Attacks. Gartner Inc. December 17, 2007. Acedida em 16 de Novembro de 2013. Informação disponível para consulta em:

http://www.gartner.com/newsroom/id/565125

Storm,Darlene (2013) -Hacker uses an Android to remotely attack and hijack an airplane. Computerworld.com. 10 de Abril. Acedida em 12 de Maio de 2013. Informação disponível para consulta em:

http://blogs.computerworld.com/cybercrime-and-hacking/22036/hacker-uses-android-remotely-attack-and-hijack-airplane

Thill, Scott (2009).1948: William Gibson, Father of Cyberspace. Revista Wired, 03.17.09, também acedida em 8 de março de 2013, disponível em:

http://www.wired.com/science/discoveries/news/2009/03/dayintech_0317

Titevski, Valery (2011a). Ex-chief engineer of Siberian power plant charged with safety violations. RIA Novosti. 2011. Acedida em 15 de Fevereiro de 2013. Informação disponível para consulta em:

http://en.rian.ru/russia/20110114/162142738.html

Titevski, Valery (2011b). Investigators complete Siberian power plant disaster probe. RIA Novosti. Acedida em 15 de Fevereiro de 2013. Informação disponível para consulta em:

http://en.rian.ru/trend/dam/

Universidade da Beira Interior. "Noção de software. As aplicações WORD e EXCEL". Acedida em 7 Novembro de 2012 disponível para consulta em:

http://www.di.ubi.pt/~cbarrico/Disciplinas/Informatica/Downloads/Capitulo3.pdf

World Economic Forum. Acedida em 7 de março de 2013. Disponível para consulta em:

http://www.weforum.org/reports/global-risks-2012-seventh-edition

7. ANEXOS

7.1. Principais funções das camadas do modelo OSI [102]

Aplicação

- Login & Password;
- Forma de representar informação comum;
- Assegurar o início, desenvolvimento e fim das aplicações;
- Transferência de ficheiros, acesso e manutenção;
- Formas de representação padrão;
- Tratamento de mensagens;
- Transferência de documentos;
- Acesso a bases de dados;
- SVA (videotex, E-mail, EDI, etc.) ;
- Manutenção de sistemas;
- Protocolos industriais.

Apresentação

- Transferência de dados para tipos de dados comuns (ASCII).

Sessão

- Passa endereços para locais nominativos;
- Estabelece e termina ligações;
- Transfere os dados;
- Controla o diálogo.

Transporte

- Passagem de informação do início até ao destino;
- Multiplexagem;

102 Fonte: Monteiro, Edmundo, Boavida Fernando (2011).Engenharia de Redes Informáticas. 10ª Edição Lisboa. FCA - Editora Informática.

- Controlo de fluxo.

Rede

- Direciona pacotes de informação;
- Estabelece a rota mais adequada;
- Providência os endereços;
- Controla o tráfego de rede;
- Reconhece prioridades;
- Envia informação na ordem correta.

Dados

- Garante a integridade dos dados;
- Adiciona marcas de fim e início de mensagens;
- Fornece algoritmos de deteção e correção de erros;
- É responsável pela transparência dos dados;
- Fornece métodos de acesso à rede.

Física

- Trata tensões e impulsos elétricos;
- Especifica cabos, conectores e interfaces;
- Providência o contínuo fluxo de bit´s através do meio de transmissão.